IP-ВИДЕОНАБЛЮДЕНИЕ ДЛЯ IT-СПЕЦИАЛИСТОВ

Горбунова Юлия Сергеевна
старший менеджер по развитию бизнеса,
Кравцов Михаил Юрьевич
инженер по отраслевым решениям
Milestone Systems

ЦЕЛЬ ДАННОГО МАТЕРИАЛА — СФОРМИРОВАТЬ У СОТРУДНИКОВ IT-ПОДРАЗДЕЛЕНИЙ ПРЕДСТАВЛЕНИЕ О ВОЗМОЖНОСТЯХ СОВРЕМЕННЫХ СИСТЕМ ЦИФРОВОГО ВИДЕОНАБЛЮДЕНИЯ (ИЛИ IP-ВИДЕОНАБЛЮДЕНИЯ) И РАССКАЗАТЬ ОБ ОСОБЕННОСТЯХ ИХ ЭКСПЛУАТАЦИИ И ОБСЛУЖИВАНИЯ.

Цифровое видеонаблюдение уже давно стало неотъемлемой частью IT-инфраструктуры предприятия. IT-сотрудники должны не только заниматься обслуживанием, но и принимать активное участие в выборе системы и формировании требований. Поэтому мы рекомендуем быть проактивными — настаивать на участии в процессе выбора системы.

В данной статье мы расскажем о том, на что обращать внимание при выборе системы видеонаблюдения, а также как ее эксплуатировать.

ДОВЕРЯЙ, НО ПРОВЕРЯЙ

Итак, представим ситуацию: в организации назрела необходимость построения системы безопасности на одном из объектов (офисе, магазине, заводе и т.п.). И сотрудников технического подразделения привлекают для участия в проекте наравне с представителями служб безопасности. И от тех, и от других требуются компетенции, обусловленные знаниями особенностей объекта и опытом решения аналогичных задач (защита и администрирование сетевых систем) в прошлом.

Тут самое время задуматься, что имеющийся опыт не всегда является в подобных вещах верным союзником. Технологии, как банально бы это не звучало, не стоят на месте. Надежные решения, зарекомендовавшие себя в прошлом, могут устареть или перестать быть эффективными на фоне современных аналогов или неочевидных специфических особенностей.

Современное IP-наблюдение находится на стыке сфер технической безопасности и информационных технологий, обладая при этом своими уникальными специфическими признаками и чертами. Именно эта специфика не позволяет, на наш взгляд, однозначно применять подходы, принятые в каждой из областей.

Первое, что нужно знать об IP-видеонаблюдении сегодня — это то, что вы с очень большой вероятностью чего-то не знаете об IP-видеонаблюдении. Без лишнего философствования это утверждение призвано подчеркнуть важность профессионализма технических специалистов Исполнителя, которым делегируется формирование облика системы безопасности на всех этапах проекта. Именно эти люди держат руку на пульсе динамично развивающейся в последние годы отрасли и способны подобрать оптимальное и, что немаловажно, актуальное решение для поставленной задачи.

Не следует забывать, что конечное решение всегда является результатом коллективной ответственности. Заказчик в лице тех же представителей службы безопасности и IT-подразделений, вовремя не задавший нужные вопросы, рискует получить в свое распоряжение результат, не соответствующий ожиданиям.

Во избежание подобной ситуации в очередной раз хочется призвать к ведению плодотворного диалога с Исполнителем. Воспринимайте его специалистов как союзников и проводников в мир систем безопасности. В то же время, проверяйте

информацию, которую предоставляют Исполнители: задавайте вопросы, просите рассказать об уже реализованных проектах, сопоставляйте и тщательно анализируйте информацию. Данная статья может также служить памяткой о том, на что обращать внимание при выборе системы.

СЕГОДНЯ И ЗАВТРА

Полезно для начала ответить для себя на ряд вопросов:

- Что будет с создаваемой сегодня системой «через 5 лет»?
- Что произойдет в случае, если я захочу добавить/заменить камеры?
- Чего следует ожидать при возникновении потребности в увеличении масштаба системы?
- Какие выгоды еще можно извлечь из системы помимо основной задачи обеспечения безопасности?

Задумывайтесь о сроках службы, особенностях обслуживания, развития системы. Одним словом, задумывайтесь о владении системой.

Нередки ситуации, когда у заказчиков имеется много филиалов с разрозненными системами безопасности. В настоящий момент рынок видеонаблюдения может предложить достаточное количество решений, которые бы могли удовлетворить потребность объединения нескольких территориально распределенных объектов в единую централизованную систему мониторинга.

Построение иерархических систем также может быть осуществлено несколькими способами. Например, системы видеонаблюдения мелких филиалов с более простым в функциональном плане ПО могут быть подключены к некой главной системе. Операторы и администраторы такой главной системы при этом имеют возможность централизованно обращаться к любому дочернему узлу этого иерархического древа подключенных систем для настройки любой камеры или просмотра трансляции или архива.

Цифровое видеонаблюдение сегодня можно представить в виде сочетания нескольких ключевых компонентов:

- среда передачи данных или попросту сеть;
- подсистема хранения;
- система управления видеонаблюдением (ПО);
- устройства захвата видео и прочих данных (камеры, микрофоны и различные датчики);
- серверы (в том числе виртуализация и аппаратное ускорение);
- интеграционные решения.

Мы считаем, что «софт — всему голова». Он позволяет обеспечить централизованное управление и способен раскрыть потенциал как каждого отдельного компонента, так и всей системы целиком. Правильное сочетание компонентов и распределение мощностей между ними дает простую в обслуживании и масштабируемую в перспективе систему.

СИСТЕМА ПЕРЕДАЧИ ДАННЫХ

Никаких откровений в этом вопросе нет. Наилучшая производительность сетевой инфраструктуры по-прежнему достигается при использовании сетевого оборудования одного вендора. Случается, что инженеры в своей практике сталкиваются с яркими исключениями, но это, как правило, обусловлено наличием откровенно неудачных моделей. В случае системы видеонаблюдения важно помнить о необходимости поддержки оборудованием технологии Power on Ethernet (PoE), способности обрабатывать большое количество сетевых запросов, при этом непрерывно «прокачивая» через себя большие объемы потоковых данных.

При решении отдельных задач иногда возникает необходимость использования видеонаблюдения на нестабильных каналах связи с малой пропускной способностью. Уточняйте, может ли комплексное решение поддерживать работу в таких своего рода экстремальных условиях.

СИСТЕМЫ ХРАНЕНИЯ

Опыт подсказывает, что в 80% случаев проблемы функционирования систем IP-видеонаблюдения связаны с подсистемой хранения. Будь то неверно подобранное оборудование, ошибки на этапе проектирования хранилища или неудачно выбранная конфигурация дисков, результат зачастую один — система не «переваривает» весь «скармливаемый» ей объем видеоданных.

Опыт также подсказывает, что проблемы подсистемы хранения зачастую обусловлены естественным стремлением сэкономить. С учетом того, что видеоданные могут быть использованы не только для задач оперативного реагирования, но и для доступа к порой весьма ценному архиву при анализе самых различных событий, хотелось бы обеспечить их максимальную сохранность и защищенность. Хочется обратить внимание, что экономия на данном компоненте системы может обернуться крайне неприятными ситуациями. Это утверждение распространяется не только на оборудование, но и на программные компоненты, которые управляют этим оборудованием или непосредственно взаимодействуют с ним.

Чтобы инвестиции в организацию качественного и надежного хранилища окупились, современные системы управления видеонаблюдением предлагают различные решения, продлевающие срок службы дисковых массивов.

Одним из подобных решений является буферизация видеопотоков в оперативной памяти сервера, выполняющего роль видеорегистратора. Данная функция в сочетании с правильно настроенной детекцией движения (как серверным, так и камерным ее вариантом) или более сложными запрограммированными реакциями на внешние события позволяет существенно снизить нагрузку на подсистему хранения. Изначально накопленные в буфере более быстрой оперативной памяти и тем самым миновавшие промежуточное кеширование на дисковой подсистеме обрабатываемые видеопотоки будут записаны только в ситуациях, когда система установит необходимость подобной записи.

Немаловажным аспектом является балансирование нагрузки между компонентами системы. Нередко на этапе проектирования системы крайне сложно или даже невозможно предсказать реальную нагрузку на каждый сервер управления записью. Возможность перераспределения нагрузки в процессе работы системы путем перенаправления отдельных потоков с одного сервера на другой может существенно упростить доводку и оптимизацию системы после постановки ее «на боевое дежурство».

Не стоит забывать об отказоустойчивости. Здесь балом правят стандартные практики, прекрасно зарекомендовавшие себя в IT-сфере. Использование RAID-контроллеров и резервного оборудования. Автоматизация механизмов отказоустойчивости в целом реализована на достаточно высоком уровне. Современные системы позволяют активно использовать кластеризацию, холодное и горячее резервирование для узлов системы видеонаблюдения.

Также важно убедиться, учтены ли рекомендации производителей при первоначальной подготовке подсистемы хранения. Производители оборудования и ПО нередко делятся информацией по конфигурированию своих систем для достижения оптимальной производительности.

ВИРТУАЛИЗИРУЙ ЭТО!

Несмотря на то, что использование технологий виртуализации уже давно и прочно вошло в повседневную жизнь организаций и IT-профессионалы достаточно хорошо освоили тонкости и нюансы построения и эксплуатации масштабных виртуальных систем, хочется указать на некоторую специфику использования виртуальных машин для размещения компонентов системы видеонаблюдения.

Как правило, в системе цифрового видеонаблюдения возможно выделить узлы (сервисы, программные модули и т.п.), отвечающие за общее управление и/или регистрацию и обработку системных событий, и узлы, отвечающие за непосредственное взаимодействие с видеопотоками и их запись. Практика показывает, что первые, как правило, по-

требляют меньшее количество системных ресурсов и в конечном счете подлежат виртуализации с сохранением всех ее основных преимуществ. Основным преимуществом для IP-видеонаблюдения, пожалуй, является возможность практически мгновенного восстановления виртуальной машины после перезагрузки или аварийного останова.

С другой стороны, хочется отметить еще одно обстоятельство. Прежняя практика использования виртуализации для построения систем видеонаблюдения показывала снижение производительности виртуальной системы на 30% по сравнению с аналогичными мощностями физического сервера. Некоторые функции, связанные с задействованием дополнительных вычислительных мощностей графических процессоров для улучшения количественных и качественных характеристик видеонаблюдения, например, по-прежнему плохо «стыкуются» с виртуализацией.

Но ситуация постепенно улучшается. В настоящее время все большее число интеграторов рассматривают вариант построения масштабных систем видеонаблюдения на базе совершенствуемых с каждым днем виртуальных технологий.

ТЕСТИРОВАНИЕ

К сожалению, заказчики в силу разных причин уделяют недостаточно внимания вопросу тестирования. Речь идет о проверке и решений, которые они готовы приобрести, и систем, которые уже установлены на боевое дежурство. В идеальном мире системные администраторы и сотрудники IT-подразделений должны понимать, что произойдет, если завтра что-то случится, скажем, с почтовым сервером или сервером СУБД, на который «замыкается» значительная часть бизнес-сервисов, и, самое главное, какие действия необходимо будет предпринять или будут предприняты автоматически для исправления аварийной ситуации. К сожалению, в мире реальном подобные уровни компетенций и проактивности не всегда достижимы.

Точно такими же знаниями нужно обладать и об особенностях работы системы видеонаблюдения.

Наиболее удачной возможностью изучения поведения системы видеонаблюдения в любых ее состояниях, на наш взгляд, является использование пилотных инсталляций с обязательным проведением нагрузочного тестирования. Безусловно, подобный подход требует выделения определенного времени на реализацию, которое, будем объективны, не всегда просто отыскать. Но при этом вы получите представление об особенностях функционирования «кандидата» и сможете более взвешенно подойти к вопросу выбора.

Хочется затронуть один, пожалуй, до сих пор еще достаточно экзотический для отрасли безопасности способ проверки отказоустойчивости крупных распределенных систем, основанный на принципах хаосной инженерии. В 2010 году американская компания Netflix, которая является одним из крупнейших поставщиков медиаконтента для массового рынка с использованием технологий потокового видео, воплотила в жизнь любопытный принцип достижения высокой надежности своей системы. Инженеры компании создали так называемую «обезьянью армию» — набор утилит для искусственного внесения неисправностей в элементы сетевой и программной инфраструктуры своих сервисов. Обезьяньей она была названа потому, что в названии каждой утилиты присутствуют слова «обезьяна», «горилла» или «Конг» (последние взаимодействуют со структурой большего масштаба).

В основу первого разработанного приложения Chaos Monkey была положена идея об обезьяне с гранатой, которую бы в произвольный момент времени запускали в вычислительный центр с непредсказуемыми последствиями для находящегося в нем оборудования. Результатом ее действий служит произвольное отключение серверов с виртуальными машинами, на которых функционируют сервисы Netflix.

А написано это все к тому, что задачи обработки, хранения и трансляции потокового видео множеству абонентов весьма схожи с задачами управления и использования архива в видеонаблюдении. Подобный экстремальный подход, разумеется, доступен не многим и, скажем прямо, не везде возможен.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Без лишнего лукавства заметим, что полноценное раскрытие аспектов информационной безопасности (и кибербезопасности в частности) применительно к видеонаблюдению невозможно в рамках раздела данного материала. Тема заслуживает полноценного цикла отдельных статей. Настолько велик, масштабен и актуален вопрос.

Согласно отчету Nu Data Security за последние 5 лет в среднем злоумышленники получают доступ к 3,8 миллионам записям в день. Невероятная цифра, которая красноречиво свидетельствует о масштабе проблемы.

Все говорят о кибербезопасности только в разрезе безопасности камер, но мы хотим обратить внимание на то, что защищать нужно абсолютно все узлы системы видеонаблюдения. И в данном случае ПО, используемое для управления видеонаблюдением, играет ключевую роль, поскольку должно служить ядром этой защиты, соответствуя стандартам цифровой безопасности.

АНАЛИТИКА

Под аналитикой сейчас понимаются практически любые решения, так или иначе связанные с обработкой видеоданных. С одной стороны справедливо будет утверждать, что развитие технологий, их адаптация к специализированным задачам и растущий интерес разработчиков ПО к рынку безопасности действительно приводят к постоянному совершенствованию предлагаемых на рынке решений и, как следствие, улучшению их качества в целом. С другой стороны, хочется лишний раз подчеркнуть, что любую аналитику нужно проверять. Тем более производители сегодня, как правило, предоставляют такую возможность. Кажется, здесь уместно провести аналогию с тест-драйвом при покупке автомобиля.

Качественная аналитика выдает результат с минимальным количеством ложных срабатываний и, собственно, с минимальным количеством «промахов».

При прочих равных условиях качество аналитики также зависит от качества оптимизации специализированных алгоритмов (насколько быстро работает алгоритм и как много системных ресурсов он потребляет). Число решений на рынке растет с каждым днем, и возможность выбора решения, удовлетворяющего текущим потребностям, является большим преимуществом.

Система видеонаблюдения должна позволять вам протестировать аналитические продукты от разных производителей перед выбором «того самого» верного решения.

ЗАКЛЮЧЕНИЕ

Мы постарались рассмотреть моменты, на которые следует обратить внимание. Не бойтесь быть придирчивыми и задавать вопросы. Желаем, чтобы затраченные при выборе усилия не пропали зря и вы получили ту систему, которая будет верной службой защищать ваши интересы, ваш бизнес и просто будет радовать вас долгое время.

ПЕРЕЧЕНЬ КРАТКИХ СОВЕТОВ ДЛЯ ЗАКАЗЧИКА

1. *Узнавайте о решениях, которые вам нужны.*
2. *Ведите диалог с интегратором для поиска оптимальных решений, отвечающих Вашим задачам.*
3. *Настаивайте на тестовой эксплуатации предлагаемых решений в боевых условиях, чтобы минимизировать риски неверного выбора.*