Защищена ли наша телекоммуникационная инфраструктура?

Высокие технологии могут решить уникальные проблемы индустрии

Энди Хильверда

События 11 сентября 2001 года и сезон ураганов 2005 года проявили зависимость США от эффективной национальной телекоммуникационной инфраструктуры. Телекоммуникационные компании – это критическое звено американской инфраструктуры и ключ к защите родины в чрезвычайных ситуациях. Надежные, безотказные коммуникационные службы обеспечивают связь между аварийными бригадами, пожарными и правоохранительными органами для согласованного управления в критической ситуации.

Безопасность имеет первостепенное значение для телекоммуникационной индустрии, но компании сталкиваются с уникальными проблемами ее осуществления из-за особенностей их структуры. Компании должны обезопасить свои сети, управляя сотнями объектов в географически разобщенных регионах. Договоренность о том, у кого есть права на доступ и когда они используют это право очень важна для обеспечения безопасности работы.

Нерешенные проблемы

Постоянные проблемы управления удаленными изолированными участками в большей мере связаны с вандализмом и кражами, нежели с терроризмом. Вместе со стремительным ростом цен на медь и другие металлы, материалы, подстанции и аппаратные помещения стали главной целью для воров. Изготавливаются дубликаты ключей, и компания не имеет представления, сколько ключей используется на местах. Воры получают доступ в аппаратные помещения и крадут дорогое сетевое коммутирующее оборудование, чтобы продать за пределами США. Кабеля обдирают до металла и продают на открытом рынке. С серьезной проблемой контроля доступа сталкиваются и собственники аппаратных помещений для антенн, расположенных на крышах, которые совместно используются многими владельцами беспроводных каналов связи, занимающие части помещения. У каждого из них свои техники, которые приходят и уходят. Персоналу, обслуживающему инженерные системы здания также необходимы права на доступ. В некоторых случаях, на месте может присутствовать система видеонаблюдения или независимые видеокамеры на входе в здание. Хотя в большинстве случаев, системы идентификации лиц имеющих доступ в разные части аппаратного помещения не применяются. Собственники не представляют, сколько "утерянных и пропавших" ключей все еще используется и сколько ключей применяются в криминальных целях.

Удаленные сотовые вышки сталкиваются с подобными проблемами, но их уязвимость усугубляется изолированностью. И снова, владельцы не располагают на местах системами отслеживания техников сотового и коммутационного оборудования, которые

посещают объекты и не обеспечивают необходимый уровень контроля над выдаваемыми ключами. Другая проблема в том, что на большинстве объектов имеется навесной замок на воротах, одна или две двери в аппаратном помещении и одна дверь в помещение с генератором. Часто замки на каждой из дверей и навесной замок на воротах разных типов и производителей, что только усложняет контроль над ключами.

Это лишь некоторые из досаждающих проблем, с которыми сталкиваются компании при осуществлении стратегии защиты своих объектов. Когда компании обращают пристальное внимание на эти проблемы, они ищут системы контроля доступа, которые обеспечивают высокую степень безопасности и обладают гибкостью. Еще боле важно, что они ищут способы контроля ключей и способы регистрации контрольных записей. Сталкиваясь с огромным множеством вариантов выбора, цен и неясных преимуществ, компании должны использовать методологию для осуществления сбалансированного подхода к достижению целей безопасности и способы измерения успешности прилагаемых усилий.

План обеспечения безопасности должен быть расширяемым, чтобы позволить телекоммуникационным компаниям контролировать доступ к множеству объектов и отслеживать множество лиц. Что касается некоторых доступных на сегодняшний день решений, ниже следует обзор технологии, которую можно включить в эффективный план управления безопасностью объектов.

Высокотехнологичные устройства

Доступны системы входных дверей, использующие биометрику для аутентификации или идентификации. До недавнего времени крупные биометрические устройства были непрактичными из-за стоимости замены оборудования и установки. Кроме того, требуется огромное количество памяти для хранения биометрических данных.

Биометрическая технология используется в большом разнообразии новых продуктов для одиночной двери и отдельных решений.

Тем не менее, данной технологии необходимо повышать производительность в продуктах, разработанных для коммерческого использования.

Многоточечные цифровые системы видеонаблюдения представляют собой жизнеспособный вариант для наблюдения за аппаратными помещениями антенн, расположенных на крышах. С развитием технологии камеры становились более компактными и теперь позволяют получать изображение даже в условиях слабой освещенности. На выбор представлено большое количество продуктов, и задача сделать выбор может обескуражить – но они определенно заслуживают внимания.

Когда рассматривается вариант цифрового видео, нужно принимать во внимание ограничения пропускной способности, а видеофайлы часто имеют чрезвычайно большой размер. Пропускная способность и размер файла тесно взаимосвязаны. Цифровые сигналы изображения необходимо обработать и передать через сеть за разумный отрезок времени. Более крупные видео изображения для передачи изображения через сеть требуют большей пропускной способности.

Когда сотни камер установлены на большой территории, обычно необходим компромисс между уровнем качества изображения и частотой обновления изображения.

Развитие технологий привело к появлению устройств безопасности на основе IP для территорий, где имеется сеть, чтобы предоставить коллективное наблюдение, контроль доступа и идентификации в крупных организациях. Эта объединяющая технология включает IP камеры, IP видео серверы, средства видеоанализа и хранения. Необходимо полностью разработать IP-систему безопасности, чтобы определить стоимость всех элементов, включая

установку. Имеется ли отдельный фонд для установки? Выделены ли административные средства для эффективного управления системой после установки? Подходящая ли это технология для решения существующих проблем? Прогресс технологии предоставляет нам беспроводный видеоконтроль. Данная система объединяет питаемые от батарей камеры, датчики и GPRS связь с центральной мониторинговой станцией. Охранные сигнализации с видеоконтролем становятся более практичными, так как стоимость систем видеонаблюдения снижается, делая их более практичным решением для локальной системы безопасности. Владельцы телекоммуникационных объектов получат преимущество от беспроводных систем в случае вторжения: можно быстро определить, когда вторжение не представляет угрозы, а когда более серьезно.

Проблемы контроля ключей

Если контроль ключей и контрольные записи представляют непосредственную проблему большинства телекоммуникационных компаний, что позволит контролировать ключи? Как они могут контролировать и организовать подотчетность приходящих и уходящих субподрядчиков и техников, которые посещают их объекты?

“При работе с телекоммуникационными компаниями я увидел дикую смесь всех типов навесных замков, дверных замков и ключей. – Рассказывает Джон Свитзер, владелец компании "Trevino Lock and Key" в Эль-Паco, штат Техас. – Нигде не было одинаковых замков, и никаких способов определения рисков безопасности, так как в обороте было неизвестное количество ключей.

Компании получают контроль над ключами и эффективные методы отслеживания техников и субподрядчиков с помощью электронной запирающей системы CyberLock®.”

Уникальность системы заключается в том, что она вмещает и уже присутствующие на телекоммуникационных объектах механические и навесные замки. Механические цилиндры внутри существующих замков заменяются электронными цилиндрами, без необходимости подведения проводки. Замки и ключи сохраняют исчерпывающие контрольные записи, так что владельцы смогут узнать, когда служащие посещали их объекты. Компания Verizon Wireless внедрила электронную запирающую систему на всех своих объектах.

“Нам нужен был более полный контроль над тем, кто входит в наши здания и система, которая позволила бы нам отслеживать использование ключей. – Сообщил Джеки Джонсон, управляющий компании Verizon Wireless в Каролине. - С помощью электронной запирающей системы мы достигли целей. Теперь мы можем отслеживать служащих, выполняющих обслуживание и другие функции.”

Ключ субподрядчика можно запрограммировать на открывание множества дверных и навесных замков.

Дополнительно можно установить срок действия ключа. Электронная запирающая система поддерживает множество способов связи между оборудованием и программным обеспечением, включая использование мобильных телефонов PDA для программирования ключей по запросу в полевых условиях.

Все из упомянутых решений действительно очень действенны и их можно интегрировать в единый план, решающий всеобщие проблемы безопасности телекоммуникационных компаний. Благодаря современным достижениям технологий обеспечения безопасности, организации имеют возможность внедрения интегрированных систем, которые обеспечивают физическую защиту, отчетность и, что самое главное, контроль ключей.

Энди Хильверда. вице президент компании Videx, Inc.