УГРОЗЫ СИСТЕМЕ БЕЗОПАСНОСТИ: КАК ИМ ПРОТИВОСТОЯТЬ?

Кобзарь Виталий Анатольевич
эксперт по архитектурам систем и решений компании Schneider Electric в России

КОМПЛЕКСНЫЕ СИСТЕМЫ

СИСТЕМЫ БЕЗОПАСНОСТИ СЕГОДНЯ

За последние несколько лет системы безопасности претерпевают значительные изменения. Системы видеонаблюдения и контроля доступа последовательно перебираются с аналоговых систем и специализированных шин в IP-технологии. Данный переход обусловлен несколькими причинами: во-первых, технологии стали гораздо доступнее по сравнению с прошлым; во-вторых, они проще в эксплуатации и масштабируемости; в-третьих, IP-технологии способствуют обеспечению большей защищенности, потому как в корпоративных компьютерных сетях предъявляются более высокие требования к безопасности. Для построения инфраструктуры систем безопасности используются выделенные ресурсы структурированных кабельных систем (СКС) предприятий либо дополнительно разворачиваемые локальные сети. Кроме того, благодаря внедрению СКС мы получаем управляемое распределение потоков: чтобы не загружать системы, для управления потоками информации выделяются отдельные подсети. Использование технологи PoE-Power over Ethernet позволяет запитывать сетевые устройства непосредственно по кабелю Ethernet. Функционирование распределенной системы обеспечивает более оперативное использование уже существующей сети Ethernet и позволяет привязать один объект, обслуживаемый системой безопасности, ко второму (например, это могут быть несколько зданий одного промышленного предприятия), объединить их подсистемы в одну.

IP-технологии позволяют проще создавать интегрированные решения систем безопасности. К примеру, оператор, который работает в ситуационном центре, с помощью интегрированных систем может централизованно и оперативно получать информацию от нескольких систем в одном интерфейсе: контроля доступа, видеонаблюдения, пожарной системы. Эта интеграция удобна для быстрого реагирования при внештатных ситуациях, а также значительно упрощает процесс сбора данных при расследованиях уже произошедших событий.

УГРОЗЫ И НЕПОЛАДКИ

Неполадки в IP-системах в первую очередь могут возникать там, где при планировании всей IT-инфраструктуры не учитывались потребности в будущей системе безопасности, а IT-специалисты уже начали настройку своего оборудования (коммутаторов, маршрутизаторов) согласно требованиям СКС. В итоге, часто возникает ситуация, в которой техническим специалистам приходится внедрять IP-оборудование систем безопасности уже после введения IT-инфраструктуры в эксплуатацию, что вызывает ряд проблем: это и выделение необходимого количества IP-адресов (статических, динамических), и выделение подсетей, маршрутизация, настройка необходимых протоколов и режимов работы IT-оборудования и другое.

При запуске новых проектов, чтобы свести к минимуму возможные неполадки, огромное внимание следует обратить на этап планирования. Помимо расчета необходимого количества устройств системы безопасности надо учитывать количество и структуру подключения, выделяемого активного сетевого оборудования, возможность по его резервированию и масштабированию, режимам и протоколам его работы с учетом потребностей систем безопасности. Все требования должны быть сформулированы на момент проектирования.

Если не выполняются требования по замене стандартных паролей и нет режима безопасности подключения к сети,

система безопасности находится априори под угрозой. Всегда найдутся пытливые умы, у которых есть желание проникнуть в систему. И в этом случае они легко могут получить к ней доступ. Ведь большинство заводских паролей на оборудование и серверы можно легко отыскать на просторах Интернета. Если эта информация не изменена в системе, то высока возможность подключения к данным устройствам посторонних с дальнейшим изменением параметров. Представим ситуацию: злоумышленник нашел в сети пароль от камеры видеонаблюдения и подключился к ней. Получив доступ, он может наложить маску, изменить разрешение камеры, ухудшив его, изменить данные для подключения к ней. Далее он может вынести ценные вещи и уйти незамеченным, воспользовавшись замешательством по устранению этих изменений.

Несомненной угрозой является и утечка информации о применяемых на объекте системах безопасности, их структуры и специфики. Здесь первостепенное значение имеет человеческий фактор, ведь именно персонал – основной канал для большинства «утечек» информации. Менеджмент должен проводить строгий отбор для сотрудников, имеющих доступ к системам безопасности, и понимать, что этот человек несет большую ответственность, обладая информацией о самой структуре системы, об оборудовании, о паролях к нему.

РЕШЕНИЯ ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ

На критически важных точках доступа рекомендуется использовать несколько систем безопасности. К примеру, у пожарного выхода или у входа в серверную установлена СКУД и система видеонаблюдения. При проходе человека данный факт фиксируется в разных системах, происходит его верификация по изображению и данным в СКУД.

Интеграция систем друг с другом позволяет повысить возможность определения несанкционированного проникновения.

При установке отдельных оконечных устройств, где использование IP-технологий невозможно и приходится использовать удлинители линий, обязательно нужно обратить внимание на то, чтобы данные линии имели шифрование. Если до модуля, установленного удаленно, по IP-сетям доходит сигнал, а далее он конвертируется и передается по интерфейсам типа Wiegant, RS-232, RS-485 и т. п., которые при желании можно считать, то это создает угрозу того, что после нескольких повторений сигналов на открытие двери можно сгенерировать такой же и открыть точку доступа. Сегодняшние угрозы системе безопасности требуют, чтобы шифрование информации осуществлялось «от конца и до конца», т. е. от сервера или контроллера и до оконечного устройства.

ОБОРУДОВАНИЕ: РЕКОМЕНДАЦИИ

Главная рекомендация для построения эффективной системы безопасности – применение оборудования известных брендов, зарекомендовавших себя на рынке и проверенных временем. Такое оборудование обычно имеет необходимый функционал, а также большой запас прочности и наработки. Важно также адаптировать настройки оборудования применительно к каждой системе отдельно и не использовать настройки по умолчанию. На этапе настройки оборудования необходимо обращать внимание, какие функции защиты включены или выключены, корректировать работу данных устройств под нужды системы. Конечно, заказчики пытаются сэкономить и часто выбирают решения малоизвестных производителей, которые заявляют широкие возможности работы и функции защиты при очень заманчивой цене. Но для промышленных сетей все же рекомендуется использовать продукцию проверенных брендов. Многие появляющиеся сейчас на рынке бренды слишком «молоды» по сравнению с компаниями-экспертами рынка, данных о надежности таких устройств, их безопасности и адекватном сроке эксплуатации мало. На мой взгляд, лучше заплатить за проверенное и надежное оборудование, поговорка «Скупой платит дважды» отлично относится к этому вопросу.

ОТ ЛОКАЛЬНЫХ – К РАСПРЕДЕЛЕННЫМ

На сегодняшний день мы можем отметить, что все чаще проекты из локальных становятся распределенными. Распределенные системы безопасности – это необходимость для многих компаний или промышленных предприятий, чьи ресурсы расположены в разных офисах либо объектах, разделенных между собой географически. Более того, если предприятие разрастается, то для оборудования новых мест и производственных линий однозначно потребуется распределенная система безопасности для возможности централизованного мониторинга всей распределенной структуры.

Специфика построения систем безопасности на местах – это использование оборудования второго уровня, предназначенного для плоских сетей. При подключении в распределенные сети это будет оборудование, поддерживающее третий уровень сетей.

Резюмируя вышесказанное, можно дать следующие рекомендации по построению систем безопасности:

- Крайне необходимо размещение центрального оборудования системы/контроллеров системы в контролируемых зонах с дополнительным мониторингом точек доступа в данную зону средствами нескольких систем безопасности (СОТ, СКУД, система обнаружения вторжения). Для критических точек и зон прохода на объект также рекомендуется применять интегрированные решения двух и более систем для контроля и верификации происходящего.
- Для мест с вынужденной удаленной установкой оконечных устройств (камера, точка доступа, беспроводные датчики движения и др.) нужно использовать защищенную и скрытую прокладку проводников сигнала, при применении удлинителей линий – устройства, прошедшие сертификацию и обеспечивающие передачу зашифрованного сигнала «от конца до конца» линии. При использовании удаленного беспроводного подключения устройств – устройства с шифрованием канала и двухсторонней связью между приемником и передатчиком сигнала.
- Устройства для построения IP-систем (коммутаторы и маршрутизаторы) необходимо внедрять с выделением для СБ отдельных виртуальных подсетей (VLAN), также важно отключать неиспользуемые порты. Выделенные порты следует конфигурировать для работы в режиме защищенного доступа (Access mode) и с использованием протокола 802.1x.
- При проведении ПНР на объекте обязательно нужно произвести смену паролей доступа к системам и оконечным устройствам и хранить данные о паролях в надежном месте в строгом соблюдении правил объекта об их разглашении.
- Системы должны находиться в локальных подсетях, а для внешнего доступа в систему безопасности операторам следует использовать решения с применением технологи защиты информации (VPN, TLS, SSL) и выделенными портами для подключения к системе. При беспроводном подключении использовать шифрование данных и контроль подключения к сети с проверкой авторизации (802.1x), скрывать используемые сети.
- Хранить информацию об объекте и применяемых паролях рекомендуется в надежном месте. Немаловажно также проводить тщательный отбор персонала, который будет иметь доступ к данной информации на предмет ее хранения и нераспространения.