ТЕХНОЛОГИИ ЗАЩИТЫ ОТ ЗЛОУМЫШЛЕННИКОВ

Сильвия Стиджеман и Беренд Ян Паламба

За последние годы мы могли наблюдать быстрые изменения, происходящие как в сфере сетевых технологий, так и в экономических условиях их применения. Становилось все более очевидным, что существующие подходы к такой сфере деятельности, как системы управления безопасностью, не будут отвечать требованиям нового столетия: все тенденции указывали на необходимость создания сетевых систем с распределенным интеллектом.

Для компании Nedap это означало, что пришло время вернуться к чертежной доске и начать все сначала. В 2000 году компания Nedap запустила на рынок новую, полностью интегрированную для работы в сети платформу безопасности AEOS, которая с тех пор уже была испытана на более чем 150 серьезных объектах. Менеджер подразделения систем безопасности Беренд Ян Паламба дал нам некоторое представление о будущем систем управления безопасностью.

ДВИГАТЕЛИ РЫНКА И ТЕХНОЛОГИЙ

Разработка нового поколения систем безопасности была продиктована потребительским спросом. Она также была поддержана двумя важными техническими разработками: коммерческим использованием современных сетевых технологий, основанных на TCP/IP (Интернет) протоколе, а также все более широким применением систем распределенного интеллекта. Это открыло целый ряд чрезвычайно интересных возможностей для управления безопасностью.

ТЕОРИЯ ЭВОЛЮЦИИ

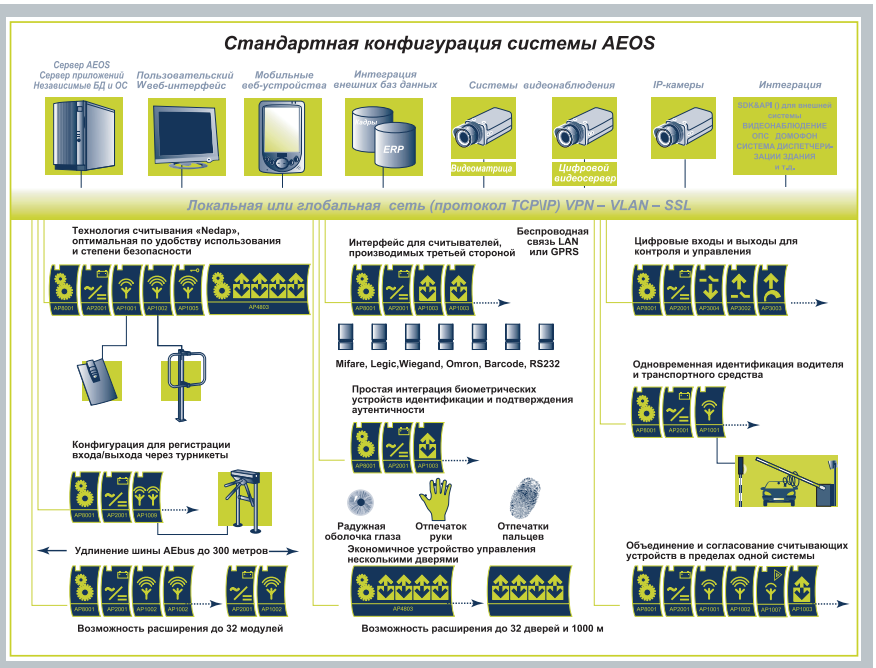
В прошлом компания могла приобрести разные системы для всех своих филиалов и впоследствии пользовалась ими в течение 15 лет. Современные решения на основе сетевых технологий позволяют постоянно изменять вашу политику безопасности в соответствии с постоянно меняющейся окружающей вас действительностью, объединяя все ваши объекты в одну центральную систему.

ДИЛЕММА

Быстрые темпы развития технологий являются основным стимулом того, что Паламба называет дилеммой управления безопасностью. Он говорит: «События развиваются настолько стремительно, что компаниям бывает сложно идти в ногу со временем. Более того, существуют ограничения, присущие существующим системам, такие как интеграция различных типов устройств чтения карт или внешних систем. Большинство систем имеют встроенные ограничения, для которых в лучшем случае можно сделать апгрейд на расширение. В связи с этим, производители систем создают множество полуэффективных методов, пытаясь взаимодействовать с новыми технологиями. На базовой структуре, которой в большинстве случаев от 10 до 15 лет!»

ПЕРЕМЕНЫ В РАБОТЕ МЕНЕДЖЕРА ПО БЕЗОПАСНОСТИ

Благодаря возможностям, присущим сетевым технологиям, широко применяемым в настоящее время, в частности одноранговым (peer-to-peer) коммуникациям, возможна организация реально распределенной интеграции устройств. Это позволяет сохранить сделанные ранее инвестиции в считыватели и карты, так как становится возможным интегрировать практически все доступные считывающие технологии, имеющиеся на рынке, в одну общую систему.



Неудивительно, что благодаря всем этим факторам основное внимание в области управления безопасности смещается от аппаратного к программному обеспечению. Такой переход к крайне гибким и расширяемым системам отражает нарастающие тенденции ухода от «костных» решений, а также ведет к практически неограниченной архитектуре системы. Другими словами – это обеспечивает более эффективную, в том числе и по стоимости, рабочую инфраструктуру для менеджеров по безопасности.

СИСТЕМЫ, КОТОРЫЕ ДУМАЮТ ЗА ВАС

Одна из ключевых особенностей современных и перспективных систем безопасности, которые в настоящее время выходят на рынок, – это распределенный интеллект – интеллект, который находится не на сервере, а в компонентах системы. Беренд Ян Паламба поясняет: «В прошлом, если вы хотели поставить камеру на дверь, где были проблемы с людьми, заходящими одновременно, вы должны были внести существенные изменения в систему. Канал связи выглядел примерно таким образом: контроллер отправлял сообщение на сервер, где оно обрабатывалось и отправлялось на видеоматрицу. Затем сообщение отправлялось на камеру, которая только после этого могла начать запись. К этому моменту, безусловно, проходило слишком много времени. Связь могла быть задержана целым рядом других факторов. Например, сервер мог иметь недостаточную свободную производительную мощность на тот момент, или сервер и матрица не смогли «найти общего языка».

Позволяя контроллеру системы самостоятельно инструктировать камеру, начать запись напрямую через сеть TCP/IP, становится возможным решить все задачи немедленно. Перемещая загрузку с сервера на контроллер, вы не только обеспечиваете быструю прямую связь, но и получаете максимальную надежность, поскольку компоненты уже не зависят от центрального сервера».

«Как могут подтвердить наши клиенты, – говорит Паламба, – изменения в мышлении и предпочтение инвестировать не в «жесткие», а в перспективные и максимально гибкие системы – это путь вперед».