KASPERSKY EMBEDDED SYSTEMS SECURITY

Решение, созданное для надежной защиты банкоматов и POS-систем

Количество киберугроз растет с каждым годом, и вместе с этим увеличивается риск атак с использованием уязвимостей нулевого дня, направленных на кражу денежных средств. Для обеспечения безопасности платежных устройств, необходимо быть на шаг впереди киберпреступников.

Защитить встроенные системы особенно трудно: обычно они распределены географически, сложны в управлении и редко обновляются. Банкоматы и POS-системы привлекают киберпреступников тем, что они непосредственно связаны с финансовыми транзакциями, выдачей наличных денег и считыванием данных банковских карт. Таким устройствам требуется направленная защита высочайшего уровня.

Стандарт безопасности PCI DSS регулирует большое число технических требований и параметров для систем, принимающих платежные карты. Однако эти требования ограничиваются лишь борьбой с вирусами, чего недостаточно для полноценной защиты от современных угроз, и последние атаки это подтверждают. Требуется новый подход: для критически важных встроенных систем нужно применять технологии контроля устройств и запрета по умолчанию, которые уже подтвердили свою эффективность в других защитных решениях.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

НИЗКИЕ ТРЕБОВАНИЯ К АППАРАТНЫМ РЕСУРСАМ

Архитектура решения позволяет ему эффективно работать даже на низкопроизводительном оборудовании: Kaspersky Embedded Systems Security обеспечивает надежную защиту, не перегружая систему.

ОПТИМИЗАЦИЯ ДЛЯ РАБОТЫ С WINDOWS® XP

Около 90% банкоматов по-прежнему используют ОС семейства Windows XP, поддержка которого прекращена производителем. Решение Kaspersky Embedded Systems Security оптимизировано для полнофункциональной работы на платформе Windows XP, так же, как и на ОС Windows 7, Windows 2009 и Windows 10 IoT.

ПОДДЕРЖКА БЕЗОПАСНЫХ ИЗОЛИРОВАННЫХ СЕТЕЙ

Базу сигнатур вредоносного ПО можно обновлять как автоматически (через интернет), так и вручную — эта возможность предусмотрена для безопасных изолированных сетей, которые зачастую применяются для банкоматов и POS-систем. При использовании сценария «Запрет по умолчанию» обновления не требуются.

ИНТЕГРАЦИЯ С ОБЛАЧНОЙ СЕТЬЮ БЕЗОПАСНОСТИ

Использование аналитических данных об угрозах, получаемых в режиме реального времени от облачной сети безопасности Kaspersky Security Network, обеспечивает максимальную эффективность технологий «Лаборатории Касперского». Благодаря этой интеграции решение защищает корпоративные системы даже от новейших угроз, включая эксплойты нулевого дня.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ

Политики безопасности, задачи обновления сигнатур и проверки на вирусы, а также мониторинг результатов — всем этим легко управлять через единую централизованную консоль администрирования Kaspersky Security Center. Всеми средствами защиты можно управлять через любую локальную консоль: это особенно важно при использовании изолированных, разделенных сегментов сети, в которые обычно объединяются банкоматы и POS-терминалы.