Как «Лаборатория Касперского» помогает защищать банкоматы Сбера на Linux-системах

kaspersky

СБЕР

Контекст

О компании

«Сбербанк»
http://sberbank.ru/
Банковский сектор

- **Крупнейший банк России по размеру активов**
- **Год основания: 1841**
- **Более 110 млн частных клиентов**
- **Универсальный банк с широкой линейкой продуктов и услуг**

«Сбербанк» – лидер российского банковского сектора, предлагающий своим клиентам высокотехнологичные сервисы и инновационные решения. Банк обладает самой обширной сетью банкоматов в стране – 39% от всех устройств.

Проблематика

Банковский сектор предъявляет особенно высокие требования к защите встраиваемых систем – банкоматов, платежных терминалов и специализированного оборудования. С точки зрения информационной безопасности у таких устройств есть свои критические особенности:

Географическая распределенность

Огромная масштабная сеть из банкоматов по всей стране требует централизованного управления безопасностью с возможностью оперативного реагирования на инциденты.

Переход на встраиваемые системы на базе Linux

Встраиваемые системы на базе Linux быстро набирают поплуярность и все чаще становятся мишенью злоумышленников. При этом выбор специализированных защитных решений для Linux куда более ограничен, чем для Windows.

Финансовые транзакции

Банкоматы обрабатывают конфиденциальные данные клиентов и совершают финансовые операции.

Количество киберугроз, направленных в том числе на банкоматы, постоянно растет. Злоумышленники разрабатывают все более изощренные методы атак, включая вредоносное ПО.

Специфика отрасли и масштаб инфраструктуры требуют комплексного подхода к защите встраиваемых систем. Банку с десятками тысяч устройств необходимо не просто установить антивирус, но и обеспечить:

- **Централизованное управление защитой всех устройств**
- **Поддержку операционных систем на базе Linux**
- **Минимальную нагрузку на маломощное оборудование**
- **Защиту от современных и неизвестных угроз**

Kaspersky Embedded Systems Security для Linux

Для внедрения было выбрано специализированное решение для защиты встраиваемых систем – **Kaspersky Embedded Systems Security для Linux**

Решение

Критерии выбора

Важнейшим требованием стала совместимость с операционными системами на базе Linux: Сбер осуществил масштабный перевод устройств с Windows на ОС собственной разработки — InterOS на базе Linux. Регулярно проводилось совместное тестирование, по результатам которого был подписан сертификат совместимости между ОС собственной разработки «Сбербанка» и Kaspersky Embedded Systems Security для Linux.

Многоуровневая защита обеспечивает комплексную безопасность за счет интеграции нескольких технологий: контроля приложений и защиты от сетевых угроз. Такой подход позволяет противодействовать широкому спектру киберугроз.

Наконец, централизованное управление через единую консоль Kaspersky Security Center оказалось критически важным для инфраструктуры такого масштаба. Возможность управления десятками тысяч устройств из одной точки существенно упрощает администрирование и позволяет оперативно реагировать на инциденты безопасности.

Ключевые возможности решения:

Контроль приложений

Режим «Запрет по умолчанию» блокирует запуск любых программ, кроме доверенных. Уникальная система работы с «белыми списками» на основе сертификатов для приложений Linux значительно снижает операционные затраты, обеспечивая при этом актуальность часто изменяемых приложений.

Контроль устройств

Решение предотвращает компрометацию системы с помощью съемных накопителей и допускает подключение только разрешенных устройств, блокируя один из ключевых векторов атак прямого доступа.

Защита от файловых угроз

Решение обнаруживает уже известные угрозы и эффективно определяет ранее неизвестные угрозы с помощью структурного и поведенческого анализа, использующего модели машинного обучения.

Защита от сетевых угроз

Решение позволяет проверять входящий сетевой трафик на действия, характерные для сетевых атак. При обнаружении попытки сетевой атаки на защищаемое устройство приложение блокирует сетевую активность со стороны атакующего устройства.

«Лаборатория Касперского» адаптировала **Kaspersky Embedded Systems Security для Linux** под собственную операционную систему Сбера на базе Linux. Это решение было разработано с учетом уникальных требований инфраструктуры банка и стало результатом тесного сотрудничества компаний. Возможность работы с кастомизированной Linux-системой банка продемонстрировала гибкость и технологическую зрелость продукта «Лаборатории Касперского».

Ход проекта

Масштаб внедрения

Команда информационной безопасности банка провела всестороннее тестирование совместимости **Kaspersky Embedded Systems Security для Linux** с собственной операционной системой, тщательно проверив все критически важные функции. Параллельно были разработаны четкие требования к защите, включающие контроль приложений по принципу «белых списков», мониторинг целостности системы, защиту от физических атак через USB-порты и обеспечение минимальной нагрузки на оборудование.

Следующим этапом стало **пилотное развертывание решения на тестовой группе банкоматов**. Это позволило проверить производительность и эффективность защиты в реальных условиях эксплуатации. В ходе пилотного проекта решение было доработано с учетом особенностей инфраструктуры банка.

После успешного завершения испытаний началось промышленное развертывание на всем парке банкоматов с планами расширения до 70 000 защищенных устройств. Команда также **прошла процесс сертификации для подтверждения соответствия решения** требованиям регуляторов и внутренним стандартам безопасности банка, получив необходимые сертификаты совместимости.

Завершающим штрихом стала **тонкая настройка параметров работы решения** для минимизации нагрузки на системы. Это позволило обеспечить **максимальную производительность** банкоматов при сохранении **высокого уровня защиты** от современных киберугроз.

Результаты

Этот проект позволяет постоянно совершенствовать технологии и подтверждает готовность решений «Лаборатории Касперского» работать в самых требовательных условиях финансового сектора.

Централизованное управление

Единая консоль управления помогает команде безопасности контролировать состояние защиты десятков тысяч устройств в режиме реального времени и оперативно реагировать на инциденты.

Масштабируемость решения

Успешное развертывание на десятках тысяч устройств подтвердило способность решения работать в инфраструктуре любого масштаба.

Выводы

Комплексный подход к защите встраиваемых систем, использование передовых технологий «Лаборатории Касперского» и тесное сотрудничество команд позволили Сбербанку усилить уровень безопасности распределенной инфраструктуры.

О решении:

Kaspersky Embedded Systems Security

Официальный сайт: