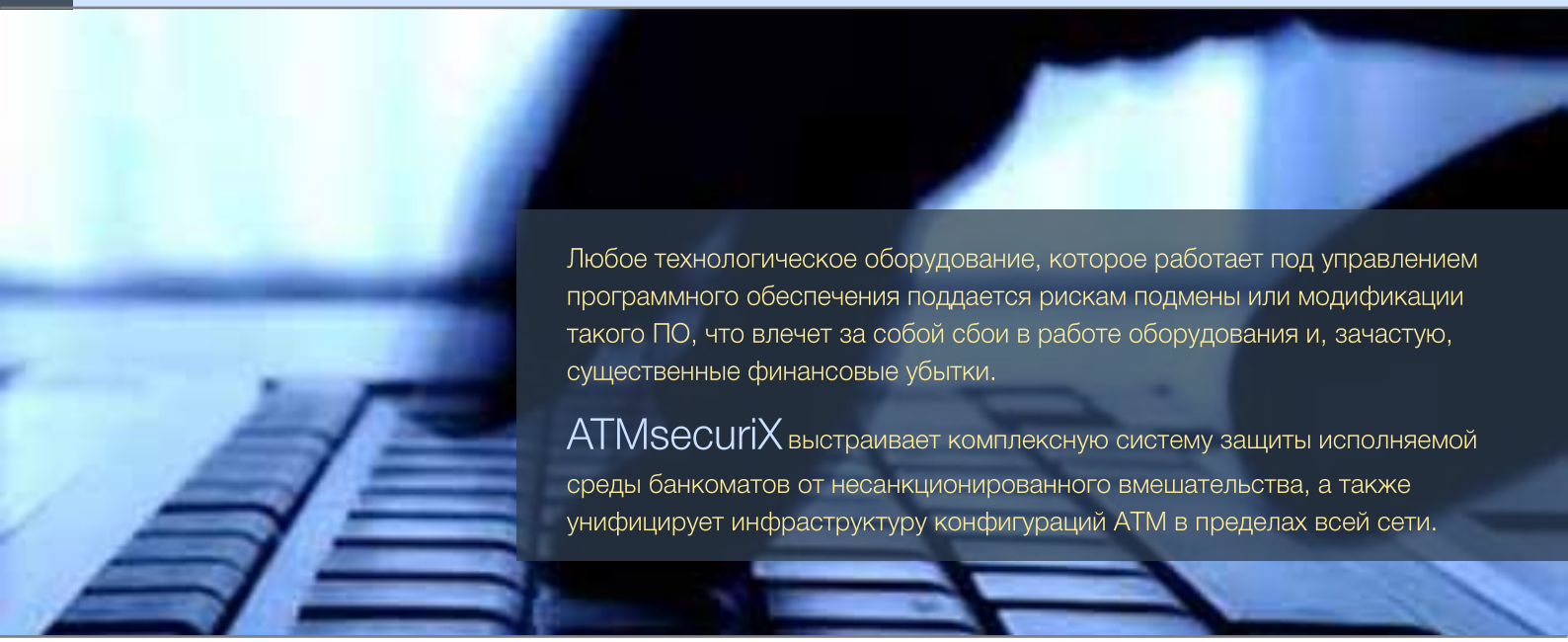
БРОШЮРА

Повышение безопасности работы сети банкоматов

ATMsecuriX

Специализированное решение для защиты программной среды банкоматов



Любое технологическое оборудование, которое работает под управлением программного обеспечения поддается рискам подмены или модификации такого ПО, что влечет за собой сбои в работе оборудования и, зачастую, существенные финансовые убытки.

ATMsecuriX выстраивает комплексную систему защиты исполняемой среды банкоматов от несанкционированного вмешательства, а также унифицирует инфраструктуру конфигураций АТМ в пределах всей сети.

За почти полвека своей истории, банкоматные технологии существенно развились по сравнению с теми, что использовались на первых этапах развития автоматизации выдачи наличных. Однако неизменным остается тот факт, что банкомат, как технологическое устройство, все так же управляется программным обеспечением, которое создается, внедряется и сопровождается человеком.

И вот, уже много десятилетий к ряду, отраслевыми специалистами регулярно создается новое программное обеспечение и внедряются новые возможности, а злоумышленники снова и снова осуществляют поиск методов несанкционированного доступа к деньгам в банкоматах и персональным данным держателей карт. И наибольшая опасность для финансового учреждения кроется в злоумышленниках-инсайдерах, которые в регламентированном режиме имеют доступ к ЭВМ банкомата.

Средства защиты банкоматов от несанкционированного доступа можно условно поделить на активные и пассивные.

К пассивным можно отнести банкоматные сейфы разных категорий защищенности, размещение банкоматов в закрытых зонах, видеонаблюдение и др. Т.е., это те средства, которые хоть и не могут остановить злоумышленника, но, все же, — усложняют его задачу.

Активные же средства, напротив, способны предотвратить неправомерные действия злоумышленника, сводя тем самым риски финансовых потерь к минимуму. Это активные антискимминговые накладки, системы окрашивания денег и т.п.

К этим же средствам относится и комплекс ATMsecuriX, который в режиме реального времени отслеживает все изменения в программной среде банкомата и предотвращает запуск несанкционированного ПО. ATMsecuriX создан с использованием уникальных компетенций в части разработки специализированного программного обеспечения для банкоматов. Это позволяет ему на равных противодействовать технологическим средствам злоумышленников-инсайдеров.

Возможности

ATMsecuriX создает уникальную инфраструктуру конфигураций банкоматов. Это позволяет не только всесторонне контролировать набор программного обеспечение на всех банкоматах сети, но и постоянно поддерживать его в эталонном состоянии.

ATMsecuriX Защита исполняемой среды банкомата

Повышение безопасности сети банкоматов с помощью ATMsecuriX, — это:

- ✓ Профиль-ориентированная защита функционального ПО
- ✓ Ограничение разового доступа к АТМ с помощью постоянно обновляемых кодов безопасности, жестко лимитированных по функциональным характеристикам
- ✓ Сокращение расходов за счет унификации программной среды на разных АТМ

ATMsecuriX упорядочивает оборот версий и модификаций функционального ПО банкоматов. Именно "прямолинейный" подход ATMsecuriX к защите банкомата обеспечивает высокий уровень противодействия злоумышленникам-инсайдерам:

- Создание профилей безопасности программного обеспечения банкоматов
- Отслеживание изменений в ПО банкомата и его отключение в случае обнаружения несоответствия профилю

Защита

В современном мире информационных технологий наиболее сложно противодействовать злоумышленникам-инсайдерам, ведь они не только имеют практически неограниченный (во всяком случае, до установки ATMsecuriX) доступ к оборудованию, но и зачастую обладают знаниями, необходимыми как для завладения деньгами и персональными данными клиентов банков, так и для сокрытия следов преступления.

Активная защита от подмены и модификации ПО банкомата злоумышленниками вместе с комплексом административных мер безопасности (разделение функций подготовки профилей безопасности и выполнение работ на банкомате, строгий учет доступа к банкоматам и оборота кодов для сессий разового доступа к оборудованию) позволяют банкам, использующим ATMsecuriX, выстроить прозрачную и надежную систему защиты от современных угроз безопасности. Более того, ATMsecuriX блокирует попытки вредоносного ПО получить контроль над исполняемыми модулями банкомата и исключает угрозы несанкционированного доступа к ресурсам АТМ: конфиденциальным данным и наличным средствам.

Преимущества

Использование ATMsecuriX, как профиль-ориентированного решения по защите банкоматов, позволяет решать не только задачи безопасности.

В процессе долгих лет своей эксплуатации терминальная сеть обычно накапливает не только разное оборудование, но и разные образцы ПО и, что особенно важно, — конфигураций банкоматов. И если с учетом первого нюанса сеть АТМ все еще может нормально функционировать, то неконтролируемые процессы в части ПО банкомата грозят не только изъянами безопасности, но и повышением расходов на ежедневную поддержку не однотипного (и часто, неучтенного) программного обеспечения.

Использование ATMsecuriX, — это:

- Стандартизация конфигураций программного обеспечения на банкоматах
- Обеспечение аутентичности исполняемых файлов функционального программного обеспечения банкомата
- Сокращение затрат на поддержку АТМ

RENOME SMART

Главный офис:
ул. Костромская, 25
Ровно, Украина, 33022

тел. / факс +380 362 69 34 27
soft@renome.ua
www.renome-smart.com