



**Kaspersky®
Embedded Systems
Security**

Leistungsstarker Schutz für Ticketautomaten und POS-Systeme, die mit Windows®-Betriebssystemen genutzt werden

Ticketautomaten, elektronische Kiosksysteme und ähnliche POS-Geräte sind aus den folgenden Gründen einem besonders hohen Risiko von Cyberangriffen ausgesetzt:

- Normalerweise wird auf ihnen eine Version der veralteten Windows XP-Betriebssystemfamilie ausgeführt.
- Es werden Finanztransaktionen auf ihnen abgewickelt.
- Sie sind geografisch verstreut und werden selten aktualisiert.
- Sie sind Teil eines internen Netzwerks.
- Sie bieten einen klassischen Einstiegspunkt für zielgerichtete Angriffe.

Als bevorzugte Ziele für Cyberkriminelle benötigen POS-Geräte wie Ticketautomaten einen extrem konzentrierten, intelligenten Schutz. Der Payment Card Industry Data Security Standard (PCI DSS) reguliert viele der technischen Anforderungen und Einstellungen für Systeme zur Abwicklung von Kreditkartentransaktionen. Die Sicherheitsvorschriften für POS-Systeme scheinen jedoch nur den Virenschutz abzudecken. Ein rein auf Virenschutz basierender Ansatz ist im Fall der aktuellen Bedrohungen von POS-Systemen aber nur von eingeschränkter Wirkung, was bei den neuesten Angriffen deutlich wurde. Die Zeit ist gekommen, Ansätze wie Gerätekontrolle und Default Deny auf Ihre kritischen Embedded Systems anzuwenden, da sich diese Technologien bereits in anderen Sicherheitskontexten bewährt haben.

Kaspersky Lab hat eine Lösung speziell für POS-Geräte einschließlich Ticketautomaten entwickelt.

Optimierte Effizienz – Integriertes Management

Mit Kaspersky Embedded Systems Security erhalten Ihre Sicherheitsteams umfassende Transparenz und Kontrolle über jeden einzelnen Endpoint.

Die Lösung ist unbegrenzt skalierbar und bietet Zugriff auf Bestandslisten, Lizenzierung, Remote-Troubleshooting und Netzwerkkontrollen, die alle über eine Konsole zugänglich sind: das Kaspersky Security Center.

Der Security Specialist kann alle Agents in einem lokalen Netzwerk über eine beliebige lokale Konsole verwalten, was insbesondere bei der Arbeit mit den isolierten und segmentierten Netzwerken der Geldautomaten und POS-Systeme wertvoll ist.

Default Deny

In den vergangenen zehn Jahren ist die Anzahl der Malware, die speziell Verkaufsautomaten angreift (darunter Tyupkin, Skimer, Carbanak und die dazugehörigen Gerätefamilien), enorm gestiegen. Die meisten herkömmlichen Antiviren-Lösungen können vor diesen hochentwickelten, zielgerichteten Malware-Bedrohungen nicht mehr ausreichend schützen. Die Default-Deny-Funktion sorgt dafür, dass ohne Genehmigung vom Sicherheitsadministrator keine anderen ausführbaren Dateien, Treiber und Bibliotheken als der Software-Schutz ausgeführt werden können.

Gerätekontrolle

Mit der Gerätekontrolle von Kaspersky Lab können Sie den Zugriff durch nicht autorisierte Geräte verhindern – so wird eine wichtige Zugriffsmethode blockiert, die von Cyberkriminellen häufig als erster Schritt bei einem Malware-Angriff genutzt wird.

Instandhaltung und Support

Wir sind in mehr als 200 Ländern mit 34 Niederlassungen weltweit tätig und bieten exzellenten Support – rund um die Uhr an jedem Tag im Jahr. Dieses Engagement spiegelt sich in unseren speziellen MSA-Support-Paketen (Maintenance-Service-Agreement) wider.

Unsere professionellen Serviceteams sind immer in Bereitschaft und stellen sicher, dass Sie aus Ihrer Kaspersky-Sicherheitslösung stets das Maximum herausholen.

Kontaktieren Sie das Kaspersky Lab Enterprise Sales Team, um mehr über die effektive Sicherung Ihrer Ticketautomaten und POS-Endpoints zu erfahren.

Geeignet für Windows XP – Windows 10 IoT

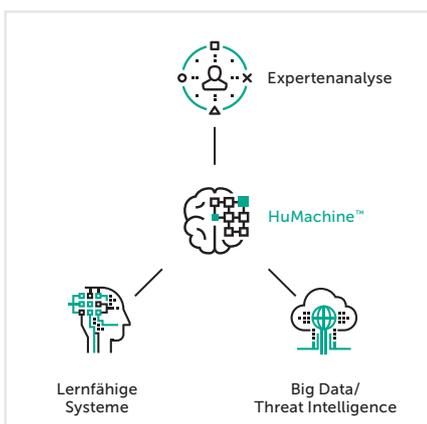
Nach zwölf Jahren lief im Januar 2016 der Support für Windows XP Embedded und im April 2016 der für Windows Embedded for Point of Service aus. Für das Betriebssystem Windows XP wird es keine weiteren Sicherheits-Updates und auch keinen technischen Support mehr geben. Kaspersky Embedded Systems Security bietet eine 100%ige Unterstützung der Windows XP-Produktfamilie.

Entwickelt für Embedded Systems Hardware

Kaspersky Embedded Systems Security bietet auch für Low-End-Systeme, die nahezu für jede POS-Hardware genutzt werden, absolute Sicherheit. Für Windows XP sind lediglich 256 MB RAM und nur 50 MB Speicherplatz auf der Festplatte des Systems notwendig. Im „bedarfsabhängigen“ Betriebsmodus nutzt das Antiviren-Modul die Hardwareressourcen nur während der manuellen oder geplanten Antiviren-Scans.

Antivirus und Kaspersky Security Network

Kaspersky Embedded Systems Security bietet einen wirksamen Virenschutz sowie regelmäßige automatische oder manuelle Updates der Malware-Signaturen, sobald diese erforderlich sind. Über die Hälfte aller auf POS-Systemen gefundenen Malware gelangt über Zero-Day-/Zero-Second-Exploits in das System. Deshalb empfiehlt Kaspersky Lab zudem die Wissensdatenbank des Kaspersky Security Network, um auf Exploits basierende Sicherheitsrisiken zu verhindern und abzumildern sowie die Reaktionszeit zu verkürzen.



Kaspersky Lab
Cybersicherheit für Unternehmen: www.kaspersky.de/enterprise-security
Neues über Cyberbedrohungen: de.securelist.com/
IT-Sicherheitsnachrichten: www.kaspersky.de/blog/b2b/

#truecybersecurity
#HuMachine

www.kaspersky.de

© 2017 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Handelsmarken und Markenzeichen sind das Eigentum ihrer jeweiligen Rechtsinhaber.