KASPERSKY EMBEDDED SYSTEMS SECURITY

Leistungsstarker Schutz speziell für kritische Bezahlungssysteme

Die Bedrohungslage hat sich exponentiell verschärft Wichtige Geschäftsprozesse, vertrauliche Daten und finanzielle Ressourcen sind einem ständig wachsenden Risiko durch Zero-Second-Attacken ausgesetzt. Um das Risiko für Ihre kritischen Finanz- und Bezahlungssysteme zu verringern, müssen Sie schlauer, besser gewappnet und besser informiert sein als die Cyberkriminellen, die es auf Sie abgesehen haben.

Insbesondere eingebettete Systeme stellen ein Sicherheitsproblem dar, da sie geographisch oft weit verbreitet und daher schwer zu verwalten sind und nur selten aktualisiert werden. Geldautomaten und POS-Systeme sind ein beliebtes Ziel für Cyberkriminelle, da sie echtes Geld und Kreditkartendaten verarbeiten. Deshalb benötigen diese ein höchst fokussiertes und intelligentes Sicherheitssystem.

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 Geldautomaten und POS-Systeme scheinen jedoch nur den Virenschutz abzudecken. Ein rein auf Virenschutz basierender Ansatz ist im Fall der aktuellen Bedrohungen von Geldautomaten und POS-Systemen jedoch nur von eingeschränkter Wirkung, was bei den neuesten Angriffen deutlich wurde. Die Zeit ist gekommen, Ansätze wie Gerätekontrolle und Default Deny auf Ihre kritischen eingebetteten Systeme anzuwenden, da sich diese Technologien bereits in anderen Sicherheitskontexten bewährt haben.

WICHTIGSTE VORTEILE DER LÖSUNG:

LOW-PERFORMANCE-HARDWARE

Kaspersky Embedded Systems Security wurde speziell für den effizienten Betrieb auf Low-End-Hardware entwickelt. Das effiziente Design bietet leistungsstarke Sicherheit, ohne dass das System überlastet wird.

FÜR WINDOWS XP OPTIMIERT

Rund 90 % der Geldautomaten laufen noch immer mit dem Betriebssystem Windows® XP, das nicht mehr unterstützt wird. Kaspersky Embedded Systems Security wurde für den Betrieb mit voller Funktionalität auf der Windows XP-Plattform sowie auf den Systemen Windows 7, Windows 2009 und Windows 10 optimiert.

FÜR ISOLIERTE GESICHERTE NETZWERKE GEEIGNET

Malware-Signaturen können über das Internet automatisch oder manuell aktualisiert werden, was für die isolierten gesicherten Netzwerke von Geldautomaten und oftmals auch anderer POS-Systeme besonders wichtig ist. Bei der Installation „Nur Default Deny" sind keine Aktualisierungen erforderlich.

LEISTUNGSSTARKE INFORMATIONEN ZUR BEDROHUNGSLAGE

Auf Basis einer einmaligen Ressource an Bedrohungsinformationen in Echtzeit entwickeln sich unsere Technologien kontinuierlich weiter, um Ihr Unternehmen auch vor den neuesten und ausgefeiltesten Bedrohungen zu schützen, Zero-Day-Exploits mit eingeschlossen. Indem Sie sich in Ihrer Sicherheitsstrategie an der weltweit führenden fortschrittlichen Erkennung von Bedrohungen orientieren, entscheiden Sie sich jetzt und in Zukunft für den besten Endpoint-Schutz. Für Ihr Unternehmen kann es keine bessere Sicherheitslösung geben.

ZENTRALISIERTE VERWALTUNG

Sicherheitsrichtlinien, Signatur-Updates, Antiviren-Scans und die Erfassung von Ergebnissen werden über eine einzige zentralisierte Verwaltungskonsole problemlos verwaltet: das Kaspersky Security Center. Alle Agents in einem lokalen Netzwerk können so über jede lokale Konsole verwaltet werden, was insbesondere für isolierte segmentierte Netzwerke, die typischerweise in Geldautomaten und POS-Systemen zum Einsatz kommen, wichtig ist.

Default Deny

In den vergangenen zehn Jahren ist die Zahl der Malware, die speziell Geldautomaten und POS-Systeme angreift (Tyupkin, Skimer, Carbanak und die dazugehörige Malware), enorm gestiegen. Die meisten herkömmlichen Antiviren-Lösungen können vor diesen hochentwickelten, zielgerichteten Malware-Bedrohungen nicht 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 USB-Speichergeräte kontrollieren, die mit der Hardware des Systems verbunden sind oder verbunden werden sollen. Indem der Zugriff auf unautorisierte Geräte verhindert wird, wird ein wichtiger Eintrittspunkt blockiert, der von Cyberkriminellen bei Malware-Attacken häufig als erster Schritt genutzt wird.

Geeignet für Windows XP – Windows 10

Nach zwölf Jahren lief am 12. Januar 2016 der Support für Windows XP Embedded und am 12. 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 alle Geldautomaten und 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 Antivirus-Modul die Hardware-Ressourcen nur während der manuellen oder geplanten Antiviren-Scans.

Antivirus und Kaspersky Security Network

Das Regelwerk des PCI DSS legt fest, dass alle Systeme, die Kredit- oder Debitkartendaten verarbeiten, über einen Virenschutz verfügen müssen, der regelmäßig aktualisiert wird. 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 Geldautomaten und POS-Systemen gefundenen Malware gelangt über Zero-Day-/Zero-Second-Exploits in das System. Deshalb empfiehlt Kaspersky Lab zudem den intelligenten Schutz, der auf der Wissensdatenbank von Kaspersky Security Network basiert, um auf Exploits basierende Sicherheitsrisiken zu verhindern und abzumildern sowie die Reaktionszeit zu verkürzen.

OPTIMIERTE EFFIZIENZ – INTEGRIERTES MANAGEMENT

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

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

Die Sicherheitsspezialisten können 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.

INSTANDHALTUNG UND SUPPORT

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

KASPERSKY lab