



Kaspersky[®]
Embedded Systems
Security

Leistungsstarker Schutz für medizinische Geräte, die mit Windows[®]-Betriebssystemen genutzt werden

Sicherheit ist sowohl für die Hersteller von medizinischen Geräten als auch Gesundheitsdienstleister ein wichtiger Gesichtspunkt. Medizinische Geräte müssen fehlertolerant, stabil und jederzeit verfügbar sein. Trotz ihrer großen Bedeutung sind die Geräte sowohl den Risiken ausgesetzt, die durch ihre Integration in das Netzwerk entstehen, als auch jenen, die speziell für Embedded Systems gelten, auf denen sie basieren.

Ein rein auf Virenschutz basierender Ansatz ist im Fall der aktuellen Bedrohungen von Embedded Systems, zu denen auch medizinische Geräte gehören, nur von eingeschränkter Wirkung, was bei den neuesten Angriffen deutlich wurde.

Eine effektivere Lösung, und dies gilt insbesondere dort, wo Stabilität und Kontinuität von so ausschlaggebender Bedeutung sind, besteht in einer Kombination von Default Deny und Gerätekontrolle. Diese Technologien bieten darüber hinaus effektiven Schutz vor Angriffen durch Insider, die in dem geschäftigen und belebten Alltag von Krankenhäusern nie auszuschließen sind.

Kaspersky Lab hat eine Lösung speziell für medizinische Geräte mit Embedded Windows-Betriebssystemen entwickelt.

Optimierte Effizienz – Integriertes Management

Mit Kaspersky Embedded Systems Security erhalten Ihre Sicherheitsteams umfassende Transparenz und Kontrolle über jedes Embedded Systems. Die Lösung ist hoch skalierbar und bietet Zugriff auf Bestandslisten, Lizenzierung, Remote-Troubleshooting und Netzwerkkontrollen, die alle über eine Konsole zugänglich sind, das Kaspersky Security Center. Sicherheitsspezialisten können alle Agents in einem lokalen Netzwerk über eine beliebige lokale Konsole und Kommandozeile verwalten, was insbesondere in isolierten und segmentierten Embedded Systems sowie für das Patch Management von Betriebssystemen und Middleware hilfreich ist.

Default Deny

In den vergangenen zehn Jahren ist es zu einer Zunahme der Malware gekommen, die speziell für den Angriff auf Embedded Systems entwickelt wurde.

Die meisten herkömmlichen Antiviren-Lösungen alleine bieten keinen ausreichenden Schutz mehr vor diesen hochentwickelten, zielgerichteten Malware-Bedrohungen. Die Default-Deny-Funktion sorgt dafür, dass ohne Genehmigung vom Sicherheitsadministrator keine anderen ausführbaren Dateien, Treiber oder Bibliotheken als der Software-Schutz ausgeführt werden können. Das zentrale Firewall-Management bietet zusätzliche hochmoderne Sicherheitsoptionen.

Gerätekontrolle

Mit der Gerätekontrolle von Kaspersky Lab können Sie den Zugriff durch nicht autorisierte USB-Wechseldatenträger verhindern – eine wichtige Zugriffsmethode, die von Cyberkriminellen häufig als erster Schritt bei einer Malware-Attacke genutzt wird. Interne CD/DVD-Laufwerke können zentral gesteuert werden, selbst wenn sie sich außerhalb der Domäne befinden.

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 Maintenance-Service-Agreement(MSA)-Support-Paketen wider.

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

Kontaktieren Sie das Kaspersky Lab Enterprise Sales Team, um mehr über die effektive Sicherung Ihrer medizinischen Geräte auf Embedded-System-Basis zu erfahren.

Kompatibel mit Windows XP

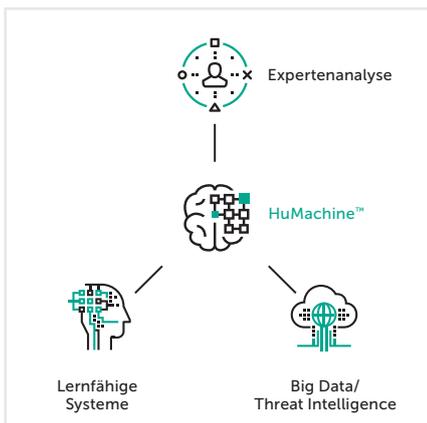
Mit dem Ende der Produktlebensdauer wurde nach 12 Jahren am 12. Januar 2016 der Support für Windows XP Embedded eingestellt. Für das Betriebssystem Windows XP wird es keine weiteren Sicherheitsupdates und auch keinen technischen Support von Microsoft mehr geben. Die meisten Sicherheitsanbieter unterstützen Windows XP-Legacysysteme nicht. Kaspersky Embedded Systems Security bietet standardmäßig eine hundertprozentige Unterstützung der Windows XP-Produktfamilie.

Entwickelt für Embedded Systems Hardware

Kaspersky Embedded Systems Security bietet selbst für eingebettete Low-End-Systeme zuverlässige 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 das Kaspersky Security Network

Bei einem Embedded System, das nur durch die Programmkontrolle geschützt wird, besteht ein erhebliches Sicherheitsrisiko durch Insider- oder Malware-Angriffe. Kaspersky Embedded Systems Security bietet einen wirksamen Virenschutz sowie regelmäßige automatische oder manuelle Updates der Malware-Signaturen, sobald diese erforderlich sind. Da die Mehrheit der Angriffe auf Embedded Systems auf die Beteiligung von Insidern zurückgeht, empfiehlt Kaspersky Lab außerdem, die Wissensdatenbank des Kaspersky Security Network zu aktivieren, um Malware-Whitelisting und Exploit-basierte Attacken zu verhindern und zu entschärfen.



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.