Kaspersky®
Embedded Systems
Security

KESS 2.0 – Neuheiten

Top-5:

Schutz des Arbeitsspeichers

Schutz des Prozessspeichers vor Schwachstellen

Kaspersky Embedded Systems Security schützt jetzt den Prozessspeicher vor Exploits. Ein dynamisch geladener Prozessschutz-Agent ist in die geschützten Prozesse integriert, überwacht ihre Integrität und verringert das Risiko der Ausnutzung von Schwachstellen.

File Integrity Monitor (FIM)

Überprüft Dateiänderungen, die eine Sicherheitsverletzung auf dem geschützten Computer darstellen könnten

Die Überwachung der Dateiintegrität (FIM) verfolgt Aktionen von bestimmten Dateien und Ordnern im überwachten Bereich. Sie können auch konfigurieren, dass Dateiänderungen nachverfolgt werden, während die Überwachung unterbrochen ist.

Protokollüberprüfung

Analyse der Aktivität in einem geschützten System über das Windows-Ereignisprotokoll

Kaspersky Embedded Systems Security überwacht jetzt die Integrität der geschützten Umgebung durch die Überprüfung von Windows-Ereignisprotokollen. Wenn ein anormales Verhalten festgestellt wird, das auf den Versuch eines Cyber-Angriffs hindeutet, benachrichtigt die Anwendung den Administrator. Die Lösung untersucht das Windows-Ereignisprotokoll und erkennt Verstöße anhand der vom Benutzer festgelegten Regeln oder anhand der Einstellungen der heuristischen Analyse, die von der Aufgabe zur Überprüfung der Protokolle verwendet wird.

SIEM-Integration

Export von Anwendungsprotokollen zum externen SIEM-System (Security Information and Event Management) über das Syslog-Protokoll

Kaspersky Embedded Systems Security kann jetzt Ereignisse in Anwendungsprotokollen in vom Syslog-Server unterstützte Formate konvertieren, sodass diese übertragen und von SIEM-Systemen erfolgreich erkannt werden können.

Überwachung von USB-Anschlüssen

Benachrichtigung über alle Verbindungen unterschiedlicher Gerätetypen mit einem geschützten Computer über USB-Anschlüsse

Kaspersky Embedded Systems Security kann USB-Speichergeräte überwachen. In Version 2 werden alle USB-Geräteverbindungen zur weiteren Analyse überwacht. Unangemessene USB-Nutzung kann als mögliche Angriffsquelle erkannt werden. Oder sie wird während der Vorfallsuntersuchungs- und Reaktionsprozesse erkannt.

Leistungsstarke Informationen zur Bedrohungslage

Auf der Grundlage von Echtzeit-Bedrohungsinformationen entwickeln wir unsere Technologien kontinuierlich weiter. So schützen wir auch Ihr Unternehmen zuverlässig vor hoch entwickelten Bedrohungen von heute und morgen. Auch vor Zero-Day-Exploits. 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 über eine lokale Konsole verwaltet werden, was insbesondere für isolierte segmentierte Netzwerke im Zusammenhang mit Embedded Systems wichtig ist.

Optimierte Effizienz – Integriertes Management

Mit Kaspersky Embedded Systems Security erhalten Ihre Sicherheitsteams umfassende Transparenz und Kontrolle über jeden eingebetteten Knoten.

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.

Administratoren können alle Agents in einem lokalen Netzwerk über eine beliebige lokale Konsole verwalten.

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.

Um mehr über die effektivere Sicherung von Embedded Systems zu erfahren, besuchen Sie www.kaspersky.de/enterprise.

Firewall- und CD-/DVD-Management

Aufgrund der Art einiger Angriffe auf Embedded Systems ist der Schutz vor bösartigen Insideraktivitäten von größter Wichtigkeit. Außerhalb des Domänenperimeters betriebene Embedded Systems müssen immer durch zentral verwaltete Gerätekontrollen für interne CD-/DVD- und USB-Speicherlaufwerke sowie durch eine Firewall geschützt werden.

Geeignet für Windows XP – Windows 10 IoT

Nach zwölf Jahren lief am 12. Januar 2016 der Support für Windows XP Embedded und am 12. April 2016 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.

Und noch wichtiger ist, dass die meisten führenden Anbieter von Endpoint-Sicherheit jetzt ebenfalls den Support für Windows XP einstellen. Kaspersky Embedded Systems Security wird auch in der absehbaren Zukunft eine hundertprozentige Unterstützung der Windows XP-Produktfamilie bereitstellen.

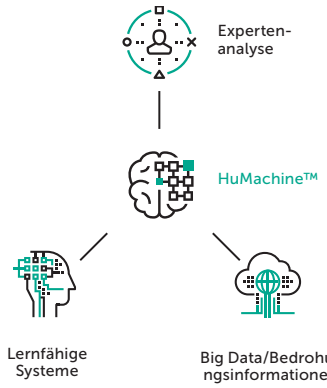
Entwickelt für Embedded Systems Hardware

Kaspersky Embedded Systems Security bietet auch für Low-End-Systeme, um die es sich bei nahezu jeder Embedded Systems Hardware handelt, absolute Sicherheit. Für Windows XP sind im „Nur Default Deny"-Betriebsmodus lediglich 256 MB RAM und nur 50 MB Speicherplatz auf der Festplatte des Systems notwendig. Das Antivirus-Modul nutzt die Hardware-Ressourcen nur während der manuellen oder geplanten Antiviren-Scans.

Antivirus und Kaspersky Security Network

Ein Virenschutz wird als optionales Modul geliefert. Die Verwendung eines klassischen „Antimalware-Ansatzes" ist aufgrund der Einschränkungen von Low-End-Hardware nicht erforderlich und in dieser besonderen Bedrohungslandschaft sowieso größtenteils ineffektiv. Wenn Kaspersky Embedded Systems Security im Gerätekontrolle- und „Default Deny"-Modus installiert ist, ist der zusätzliche Virenschutz meistens nicht erforderlich, kann aber wo erforderlich als weitere Sicherheitsstufe hinzugefügt werden.

Kaspersky Lab empfiehlt außerdem den intelligenten Schutz, der auf der Wissensdatenbank des Kaspersky Security Network basiert, um auf Exploits basierende Sicherheitsrisiken zu verhindern und zu entschärfen sowie Reaktionszeiten zu verkürzen.



Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **www.viruslist.de**
IT-Sicherheitsnachrichten: **business.kaspersky.com**

#truecybersecurity
#HuMachine

www.kaspersky.de