Kaspersky® Embedded Systems Security

Zuverlässige Sicherheit für Embedded Systems

Die Bedrohungslage hat sich exponentiell verschärft: Wichtige Geschäftsprozesse, vertrauliche Daten, finanzielle Ressourcen und die unterbrechungsfreie Verfügbarkeit von Anlagen und Systemen sind einem ständig wachsenden Risiko durch Zero-Second-Attacken ausgesetzt. Um das Risiko für Ihr Unternehmen zu verringern, müssen Sie smarter und besser gewappnet und informiert sein als Cyberkriminelle. Dabei brauchen Sie nicht mal mehr ein Ziel sein, um ein Opfer zu werden.

Heute finden sich sogenannte Embedded Systems bereits in sehr vielen Bereichen: Fahrkarten-, Geld- und Verkaufsautomaten, Kassen-Systeme im Handel, in Maschinen und Geräten der Industrie und Medizin als auch in Bereichen von Transport und Logistik. Embedded Systems stellen ein besonderes Sicherheitsproblem dar, da sie geographisch oft weit verbreitet und schwer zu verwalten sind sowie selten aktualisiert werden. Sie müssen darüber hinaus sehr fehlertolerant und -resistent sein, da sie Bargeld und Kreditkarten verarbeiten. Embedded Lösungen müssen nicht nur selbst vor Bedrohungen geschützt sein, sondern dürfen auch für Cyberkriminelle nicht als Eintrittspunkt in das Unternehmensnetzwerk zugänglich sein.

Standardmäßige Sicherheitsvorschriften für eingebettete Geräte neigen dazu, nur virenschutzbasierte Sicherheit oder Systemhärtung abzudecken, was nicht genug ist. Bestehende Sicherheitsvorschriften für eingebettete Geräte neigen dazu, nur virenschutzbasierte Sicherheit oder eine Systemhärtung abzudecken, was inzwischen nicht mehr ausreicht. Ein rein auf Virenschutz basierender Ansatz ist im Fall der aktuellen Bedrohungen von Embedded Systems nur von eingeschränkter Wirkung, was bei den neuesten Angriffen deutlich wurde. Es ist an der Zeit, bewährte Technologien wie Gerätekontrolle und Default Deny ggf. mit zusätzlichem Virenschutz für kritische Systeme anzuwenden.

Wichtigste Vorteile der Lösung

Low-End-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 sind im „Nur Default Deny"-Betriebsmodus lediglich 256 MB RAM und nur 50 MB Speicherplatz auf der Festplatte des Systems notwendig.

Für Windows XP optimiert

Viele Embedded Systems laufen noch immer mit dem Betriebssystem Windows® XP, das vom Hersteller 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.

Die meisten führenden Anbieter von Endpoint-Sicherheit stellen jetzt ebenfalls den Support für Windows XP ein. Kaspersky Embedded Systems Security wird auch in der absehbaren Zukunft eine hundertprozentige Unterstützung der Windows XP-Produktfamilie bereitstellen.

Default Deny

In den vergangenen zehn Jahren ist die Anzahl der Malware, die speziell eingebettete Systeme angreift (Tyupkin, Skimer, Carbanak und die dazugehörige Malware), enorm gestiegen. Die meisten herkömmlichen Antiviren-Lösungen können vor diesen hochentwickelten, zielgerichteten Malware-Bedrohungen nicht mehr ausreichend schützen. Eine klassische Malwareschutzlösung ist gegen die vielen gezielten Bedrohungen, die nicht auf Malware basieren, sondern Insider-Middleware mit einem anderen Angriffsansatz verwenden, nicht wirksam. 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 USB-Speichergeräte kontrolliert werden, die mit der Hardware des Systems verbunden sind oder verbunden werden sollen. Indem Sie den Zugriff auf unautorisierte Geräte verhindern, blockieren Sie einen wichtigen Angriffsvektor, der von Cyberkriminellen bei Malware-Attacken häufig als einer der ersten Schritte genutzt wird.

Alle USB-Geräteverbindungen werden überwacht und analysiert, sodass unangemessene USB-Nutzung als mögliche Angriffsquelle während der Vorfallsuntersuchungs- und -reaktionsprozesse identifiziert werden kann.

SIEM-Integration

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

Schutz des Arbeitsspeichers

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.

Zentralisierte Verwaltung

Sicherheitsregeln, 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 isoliert segmentierte Netzwerke im Zusammenhang mit Embedded Systems wichtig ist.

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.

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

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 sollten immer durch zentral verwaltete Gerätekontrollen für interne CD-/DVD- und USB-Speicherlaufwerke sowie durch eine Firewall geschützt werden.

Überwachung der Dateiintegrität

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

Protokoll-Audit

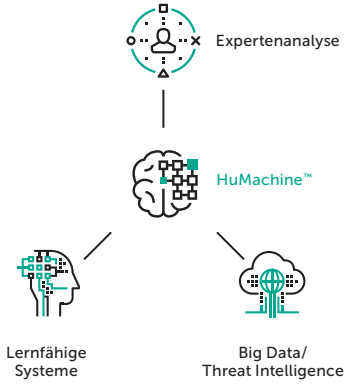
Kaspersky Embedded Systems Security überwacht die Integrität der geschützten Umgebung durch die Überprüfung von Windows-Ereignisprotokollen. Wenn ein anormales Verhalten festgestellt wird, das auf den Versuch eines Cyber-Angriffs hindeutet, benachrichtigt die Anwendung den Administrator.

Die Lösung untersucht das Windows-Ereignisprotokoll und erkennt Verstöße anhand der vom Benutzer festgelegten Regeln oder anhand der Einstellungen der heuristischen Analyse.

Antivirus und Kaspersky Security Network

Ein Virenschutz wird als optionales Modul geliefert. Die Verwendung eines klassischen „Nur-Anti-Malware-Ansatzes" ist aufgrund der Einschränkungen von Low-End-Hardware unpraktisch und in dieser einmaligen 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-security**
Neues über Cyberbedrohungen: **de.securelist.com**
IT-Sicherheitsnachrichten: **www.kaspersky.de/blog/b2b**

#truecybersecurity
#HuMachine

www.kaspersky.de