KASPERSKY EMBEDDED SYSTEMS SECURITY

Umfassende Sicherheit entwickelt 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: Geldautomaten, Fahrkarten- und andere Verkaufsautomaten, POS-Systeme im Handel, in Maschinen und Geräten der Industrie und Medizin und auch in Bereichen von Transport und Logistik. Embedded Systems stellen ein Sicherheitsproblem dar. Im Einsatz an meist geografisch verteilten Standorten sind sie meist schwer zu administrieren. Wenn dann noch eine unzureichende oder schlecht verfügbare Netzanbindung vorhanden ist, werden Aktualisierungen aufwändig und schwer. Embedded Lösungen müssen nicht nur selbst vor Bedrohungen geschützt sein, sondern dürfen auch für Cyberkriminelle nicht als Eintrittspunkt in das Unternehmensnetzwerk zugänglich sein.

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 wo erforderlich mit einem zusätzlichen Virenschutzmodul 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 OPTIMIERT
Viele Emedded 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.

FÜR ISOLIERT GESICHERTE NETZWERKE GEEIGNET
Malware-Signaturen können über das Internet automatisch oder manuell aktualisiert werden, was für die isoliert gesicherten Netzwerke von Embedded Systems besonders wichtig ist. Mit der Installation „Nur Default Deny" sind keine Aktualisierungen erforderlich.

LEISTUNGSSTARKE INFORMATIONEN ZUR BEDROHUNGSLAGE
Auf der Basis von stets aktuellen Bedrohungsinformationen in Echtzeit entwickeln wir unsere Technologien kontinuierlich weiter. So schützen wir auch Ihr Unternehmen zuverlässig vor den Bedrohungen von heute und morgen. Auch vor Zero-Day-Exploits. Mit Kaspersky Lab setzen Sie auf einen der weltweit führenden Anbieter und auf innovative Lösungen, die Ihr Unternehmen zuverlässig schützen.

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 wichtig ist.

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.

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 alle Hardware von eingebetteten Systemen genutzt werden, 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 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 von Kaspersky Security Network basiert, um auf Exploits basierende Sicherheitsrisiken zu verhindern sowie Reaktionszeiten zu verkürzen.

OPTIMIERTE EFFIZIENZ – INTEGRIERTES MANAGEMENT

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

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.

Administratoren können alle Agents in einem lokalen Netzwerk über eine beliebige lokale Konsole und Kommandozeile 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 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 Lösungen zu erfahren, besuchen Sie www.kaspersky.com/enterprise

KASPERSKY lab