Kaspersky Embedded Systems Security

kaspersky

Zuverlässige Sicherheit für Embedded Systems (und mehr)

Eingebettete Systeme sind überall, und wir haben täglich mit ihnen zu tun. Ihr Einsatz ist breit gefächert – von PoS-Systemen und Geldautomaten bis hin zu medizinischen Geräten und Tankautomaten. Mit der zunehmenden Verbreitung von Embedded Systems ziehen auch Cyberkriminelle nach und passen ihre Taktiken, Techniken und Prozeduren an die Besonderheiten dieser Systeme an.

Herausforderungen für die Sicherheit von Embedded Systems

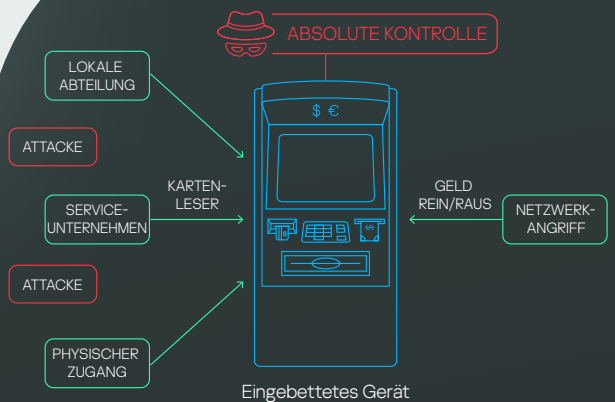
1. **Veraltete, anfällige Software.** Lange Lebenszyklen können bedeuten, dass der Support für Betriebssysteme und Apps ausläuft, deren nicht gepatchte Schwachstellen dann gezielt ausgenutzt werden.
2. **Unregelmäßig durchgeführte Sicherheitsupdates.** Auch noch unterstützte Software kann Patching-Lücken aufweisen. Die Hauptgründe für solche Verzögerungen sind Probleme bei der Aktualisierung zahlreicher geografisch verteilter Geräte oder deren Offline-Schaltung zu Wartungszwecken (und die damit verbundene zeitweise Nichtverfügbarkeit) sowie die Notwendigkeit, Updates vor der Bereitstellung zu testen.
3. **Prozesskontinuität.** Bestimmte Gerätetypen, wie z. B. medizinische Geräte, auch nur vorübergehend außer Betrieb zu nehmen, kann äußerst problematisch sein. Dies macht es noch schwieriger, Zeit für das Patching zu finden.
4. **Öffentliche Standorte.** Viele eingebettete Geräte werden im öffentlichen Raum betrieben, was das Manipulationsrisiko erheblich erhöht. Abwehrmechanismen auf Netzwerkebene bieten keinen Schutz vor einem direkten physischen Angriff auf das Gerät.
5. **Von Natur aus ein Risiko.** Da sie häufig unmittelbar an Finanzgeschäften beteiligt sind und sensible persönliche Daten verarbeiten, stellen eingebettete Geräte besonders attraktive Ziele für Cyberkriminelle dar.

Bedrohungslandschaft

Neue kriminelle Geschäftsmodelle wie Malware-as-a-Service senken die Hemmschwelle für weniger qualifizierte Angreifer. Auch wenn ältere Windows-Versionen schon lange nicht mehr unterstützt werden, werden sie dennoch weiterhin genutzt. Windows XP ist immer noch das am weitesten verbreitete Betriebssystem für eingebettete Geräte. Auf Millionen von eingebetteten Geräten und PCs laufen weiterhin alte, anfällige Betriebssysteme, die – aus den unterschiedlichsten Gründen – nicht aktualisiert werden. Diese Tatsache ist eine offene Einladung für Hacker.

Mittlerweile werden Linux-basierte eingebettete Systeme immer beliebter, und Cyberkriminelle ziehen nach, passen ihre Techniken an die Besonderheiten dieser Geräte an und entwickeln völlig neue Instrumente. Sich ausschließlich auf die in Linux bereits integrierte Sicherheit zu verlassen, ist gefährlich – denn obwohl Angreifer ihre Aufmerksamkeit erst seit relativ kurzer Zeit auf Linux-basierte Embedded Devices richten, holen sie die verlorene Zeit wieder auf. Zudem gibt es im Vergleich zu den Angeboten für Windows bislang noch nicht allzu viele Cybersicherheitslösungen für Linux-basierte eingebettete Geräte.

Unternehmen müssen beim Schutz ihrer Systeme und Daten intelligenter vorgehen als je zuvor. Kaspersky Embedded Systems Security ist eine Komplettlösung, die speziell für eingebettete Systeme entwickelt wurde. Zu den Vorteilen zählen leistungsstarke Bedrohungsdaten, Opt-in Malware-Erkennung und Exploit-Prävention, umfassende Systemhärtungskontrollen und flexible Verwaltung. Die Lösung schützt ältere Systeme, die andere Anbieter meist nicht mehr unterstützen, und jetzt auch modernere Geräte, die unter Linux laufen.



Mehr als die Hälfte aller erfolgreichen Angriffe auf Embedded Systems sind auf „Insider-Aktivitäten" zurückzuführen – entweder durch Mitarbeiter oder externe Dienstleister.

Physische Angriffe

- Black-Box-Angriffe
- PIN-Pad-Änderungen/-Skimmer
- Versteckte Kameras
- Sprengungen

Softwareangriffe

- Malware-Installation per Fernzugriff/lokal
- Memory-Sniffer/BS-Angriffe
- Infektion/Austausch von Middleware

Angriffe auf Netzwerkebene

- Schwachstellen im VPN
- Bruteforce-Angriffe auf RDP
- RCE-zulassende Netzwerk-Exploits
- Installation per Fernzugriff

Embedded Systems: typische Angriffsvektoren

Herausforderungen für die Sicherheit von Embedded Systems

6 **Strenge gesetzliche Vorgaben.** Wegen der hohen Wahrscheinlichkeit, dass auf eingebetteten Geräten Finanzinformationen und personenbezogene Daten verarbeitet werden, sind die Vorgaben für ihre Sicherheit besonders hoch.

7 **Bedrohungen von innen.** Laut Daten von Kaspersky gehen mehr als die Hälfte aller erfolgreichen Angriffe auf Embedded Systems auf „Insider-Aktivitäten" zurück – entweder durch Mitarbeiter oder externe Dienstleister.

8 **Linux verbreitet sich weiter.** Eingebettete Plattformen werden immer beliebter, da sie mehr Flexibilität bieten und eine breite Palette an Konfigurationen ermöglichen. Das wissen auch Cyberkriminelle, und die Auswahl an modernen, spezialisierten Sicherheitslösungen ist im Vergleich zum Angebot für Windows sehr viel geringer.

Highlights

Optimale Sicherheit für jedes Embedded-Szenario:
Kaspersky Embedded Systems Security ist mit einem mehrschichtigen Schutz ausgestattet und kann dadurch optimale Sicherheit für Geräte mit unterschiedlichen Leistungsstufen und Implementierungsszenarien gewährleisten. Dazu gehört die Unterstützung von Plattformen, die auf verschiedenen Betriebssystemen wie Windows und Linux basieren.

Schützt sowohl ältere als auch neue Systeme
Kaspersky Embedded Systems Security wurde so optimiert, dass es auch ohne Einschränkung der Funktionalität unter Windows XP, 7, 8, 10 und 11 läuft. Kaspersky wird Windows XP auch weiterhin unterstützen, so dass die Kunden genug Zeit für ein Upgrade haben, sobald sie dazu bereit sind. Kaspersky Embedded Systems Security unterstützt auch die neuesten Architekturen mit Windows oder Linux als Betriebssystem.

Wenig Ressourcen, viel Schutz
Kaspersky Embedded Systems Security wurde speziell für den effizienten Betrieb auf Low-End-Hardware entwickelt.

Immer mehr Angriffe auf Geldautomaten und Kassensysteme
Laut Daten von Kaspersky Research hat die Zahl der Angriffe auf Geldautomaten und PoS-Systeme im Jahr 2022 deutlich zugenommen. Der Anstieg betrug 19 % im Vergleich zu 2020 und 4 % gegenüber 2021.

Hauptfunktionen

Systemhärtung (Sicherheitskontrollen). Technologien zur Systemhärtung wie Anwendungs-, Geräte- und Update-Kontrollen gewährleisten, dass ausschließlich vertrauenswürdige Anwendungen, Peripheriegeräte und Update-Quellen genutzt werden. Dadurch wird verhindert, dass nicht autorisierte Programme gestartet und ausgeführt werden, einschließlich Malware und Anwendungen, die zum Schaden der Nutzer missbraucht werden könnten.

Optionaler Malware-Schutz. Eine optional auswählbare Sicherheitsschicht erkennt bekannte, unbekannte und hochentwickelte Bedrohungen. Sie bedient sich dabei einer präzisen Erkennungslogik auf Basis lokaler oder Cloud-basierter Bedrohungsdaten sowie Heuristiken und ML-Modellen, die vor Ort oder in der Cloud ausgeführt werden.

Exploit Prevention[1]. Verhindert die Ausnutzung von Schwachstellen in laufenden Windows-Systemkomponenten und Apps von Drittanbietern und hilft besonders ausgeklügelte Angriffe abzuwehren, die z. B. die Programmkontrolle im Default Deny-Modus zu umgehen versuchen oder mit dateilosen Techniken arbeiten.

Schutz vor Netzwerkbedrohungen. Wehrt Eindringversuche in das Betriebssystem ab und schützt vor Port-Überwachung und Brute-Force-Angriffen sowie vor dem Ausnutzen von Schwachstellen im Netzwerk, um Zielgeräte zu hacken. So können Sie einen der Hauptangriffsvektoren gegen Embedded Systems effektiv abwehren.

Integritätsüberwachung und Unterstützung bei der Einhaltung von Vorgaben. Aktionen an bestimmten Registrierungsschlüsseln, Dateien und Ordnern werden mithilfe von Überwachungsfunktionen nachverfolgt, um unerwünschte Änderungen an der Registry zu unterbinden. Damit lassen sich nicht nur Malware-basierte Eindringversuche aufdecken, sondern auch direkte Zugriffe bzw. Offline-Modifikationen an kritischen Ressourcen. Solche Maßnahmen werden in Datenschutzverordnungen oft ausdrücklich empfohlen, um Unternehmen bei der Einhaltung von Compliance-Vorschriften zu unterstützen.

Unterstützt leistungsschwache und veraltete Systeme. Unterstützt auch leistungsschwache eingebettete Systeme, die auf veralteter Hardware und unter nicht unterstützten Betriebssystemen laufen, bis hin zu Windows XP SP2. Der sichere Betrieb älterer Geräte oder Legacy-Desktops bleibt gewährleistet, bis Sie für das Upgrade bereit sind.

Protokollüberprüfung[1]. Um mögliche Sicherheitsverletzungen zu erkennen, werden die Ereignisprotokolle von Windows überwacht und analysiert. Wenn ein anormales Verhalten festgestellt wird, das auf einen versuchten Cyberangriff hindeutet, benachrichtigt das Programm den Administrator.

Flexible Verwaltung – lokal oder in der Cloud. Je nach Anforderungen können Sie Ihre eingebetteten Systeme zusammen mit anderen Kaspersky-Lösungen entweder über einen lokalen Verwaltungsserver oder als SaaS mit der Kaspersky Security Center SaaS-Cloud-Konsole verwalten. Während die lokale Verwaltung vor allem bei besonderen Anforderungen an den Datenschutz geeignet ist, spart die vom Anbieter betriebene SaaS-Konsole in der Cloud sowohl CAPEX als auch OPEX, denn sie ermöglicht einen schnelleren Einstieg in sichere Arbeitsprozesse und erfodert geringeren Wartungsaufwand.

[1] nur für Windows

Firewall-Management. Die Firewall des Betriebssystems kann direkt über das Kaspersky Security Center konfiguriert werden, sodass die Verwaltung lokaler Firewalls bequem über eine einzige, einheitliche Konsole erfolgen kann. Dies ist besonders wichtig, wenn sich Embedded Systems außerhalb der Domäne befinden und die Einstellungen der Windows-/Linux-Firewall nicht zentral konfiguriert werden können.

Geringe Toleranz bei der Konnektivität. Da viele Arten von eingebetteten Geräten an abgelegenen Standorten aufgestellt sind, ist eine schlechte Konnektivität – aufgrund von schlechter Mobilfunkabdeckung, Störungen durch nahe gelegene Funkquellen usw. – nicht ungewöhnlich. Kaspersky Embedded System Security bleibt auch bei sehr geringer Bandbreite stabil und bietet auch bei längerer Unterbrechung der Verbindung zuverlässigen Schutz.

Professional Services und Premium Support

Die ordnungsgemäße Wartung einer Sicherheitslösung über den gesamten Lebenszyklus hinweg ist an sich schon schwierig, aber die Besonderheiten von Embedded Devices, die sie von normalen Endpoints unterscheiden, erschweren die Aufrechterhaltung der Sicherheit zusätzlich. Kaspersky Professional Services bietet Unterstützung in jeder Phase dieses Lebenszyklus, von der Bereitstellung und Aktualisierung über die Konfiguration und Leistungsoptimierung bis hin zur Migration auf neuere Hardware. Und unser Premium-Support garantiert den bevorzugten Zugang zu fachkundigen Problemlösungen durch einen persönlichen und hochqualifizierten technischen Kundenbetreuer.

Verwandte Produkte und Services

Kaspersky Threat Intelligence
Eine vielseitige Auswahl an Diensten, die einen umfassenden Überblick über Cyberbedrohungen für Ihr Unternehmen bieten, indem sie unterschiedliche Threat Intelligence-Quellen, Bedrohungsdaten und interne Forschungsergebnisse unserer Sicherheitsexperten kombinieren.

Payment Systems Security Assessment: Durch eine umfassende Analyse Ihrer Geldautomaten und Kassengeräte erhalten Sie ein klares Bild Ihrer aktuellen Sicherheitslage, damit Sie den Schutz weiter verstärken, Konfigurationen optimieren und Sicherheitslücken schließen können.

Kaspersky Endpoint Security for Business: Weltweit anerkannte Endpoint Protection-Plattform, die Ihre Endpoints, Server, Workstations und Mobiltelefone mit einer häufig getesteten und vielfach ausgezeichneten Sicherheitslösung schützt. All dies wird über eine einzige Konsole verwaltet.

Branchen

- Finanzdienstleistungen
- Transport und Tourismus (Ticket-Service)
- Einzelhandel
- Restaurants und Gastgewerbe
- Gesundheitswesen
- Behörden und nicht-kommerzielle Betriebe
- Unterhaltung

Geräte

- Geldautomaten
- Ticketautomaten
- Zapfsäulen
- Kassen
- POS-Geräte
- Medizinische Geräte
- Ältere Endpoints
- Spielautomaten

Branchen, die eingebettete Geräte verwenden

Cyber Threats News: securelist.com
Kaspersky-Technologien: kaspersky.com/technowiki
IT Security News: business.kaspersky.com
IT-Sicherheit für SMB: kaspersky.com/business
IT-Sicherheit für Großunternehmen: kaspersky.com/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sicherere Welt schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren **Zukunft** bei.

Erfahren Sie mehr unter kaspersky.de/about/transparency

Proven. Transparent. Independent.