Kaspersky Embedded Systems Security

kaspersky

Sicurezza all-in-one progettata per i sistemi integrati (e non solo)

I sistemi integrati sono ovunque intorno a noi, interagiamo con loro ogni giorno e si rivelano fondamentali nei contesti più disparati: sistemi PoS e bancomat, dispositivi medici e stazioni di rifornimento automatizzate. I criminali informatici seguono con attenzione la crescita del mercato dei sistemi integrati, affinando le loro tattiche, tecniche e procedure per adattarsi alle specificità di questi sistemi diffusi.

Sfide per la sicurezza dei dispositivi integrati

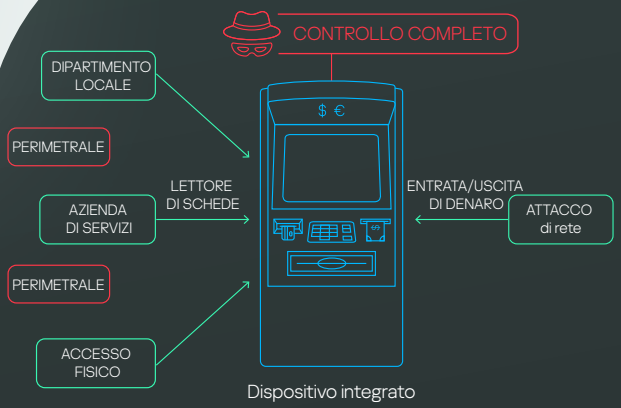
1. **Software obsoleto e vulnerabile.** Cicli di vita lunghi possono implicare l'esecuzione di app e sistemi operativi non supportati, contenenti vulnerabilità senza patch in attesa di essere sfruttate.
2. **Aggiornamenti di sicurezza irregolari.** Anche quando il software è ancora supportato, possono esserci lacune nell'applicazione delle patch. I problemi relativi all'aggiornamento dei dispositivi dislocati in aree geografiche diverse, che richiedono la disconnessione per essere aggiornati (creando quindi un DoS temporaneo), e la necessità di testare gli aggiornamenti prima della distribuzione contribuiscono ai ritardi nell'implementazione delle patch.
3. **Continuità dei processi.** Tenere alcuni tipi di dispositivi fuori uso anche temporaneamente, ad esempio le apparecchiature mediche, può essere molto problematico, aumentando ulteriormente l'arco temporale per l'implementazione delle patch.
4. **Posizioni pubbliche.** Molti dispositivi integrati operano in aree pubbliche, con un rischio nettamente superiore di compromissione. Le difese a livello di rete non possono proteggere dall'infezione fisica diretta del dispositivo.
5. **Natura intrinsecamente rischiosa.** Essendo spesso direttamente associati a operazioni finanziarie ed elaborando informazioni personali sensibili, i dispositivi integrati sono bersagli particolarmente attraenti per i criminali informatici.

Panorama delle minacce informatiche

Continuano a emergere nuovi modelli di business criminale come il Malware-as-a-Service, con l'obiettivo di abbassare il livello di competenze per gli aspiranti autori di attacchi. Sebbene il relativo supporto sia stato terminato da tempo, le versioni precedenti di Windows rimangono attive (Windows XP è ancora il sistema operativo più comunemente utilizzato nei dispositivi integrati). Milioni di dispositivi e PC integrati continuano a eseguire sistemi operativi obsoleti e vulnerabili che, per qualsiasi motivo, non vengono aggiornati. Insomma, un vero e proprio invito a nozze per gli hacker.

Al contempo, i sistemi integrati basati su Linux stanno rapidamente guadagnando popolarità e i criminali informatici ne stanno prendendo atto, adattando le loro tecniche e creando strumenti completamente nuovi in base alle specifiche dei sistemi integrati basati su Linux. Sopravvalutare la sicurezza intrinseca di Linux è pericoloso: sebbene gli aggressori abbiano rivolto la loro attenzione ai dispositivi integrati basati su Linux solo relativamente di recente, stanno recuperando il tempo perduto. Non aiuta il fatto che le attuali offerte di sicurezza informatica per i dispositivi integrati basati su Linux siano limitate rispetto a quelle disponibili per Windows.

Le aziende devono essere più intelligenti che mai per mantenere i propri sistemi e dati al sicuro. Caratterizzato da potente Threat Intelligence, prevenzione exploit e rilevamento malware opt-in, gestione flessibile e controlli completi di hardening dei sistemi, Kaspersky Embedded Systems Security è una soluzione di sicurezza all-in-one ideata specificatamente per i sistemi integrati. Fornisce un livello unico di protezione per i sistemi legacy, che non sono più supportati dalla maggior parte dei fornitori di cybersecurity, e ora offre anche lo stesso livello di protezione per i dispositivi più moderni che eseguono il sistema operativo Linux.



Oltre la metà degli attacchi riusciti a sistemi embedded comprende "attività di un insider" ossia da parte di un dipendente o di un provider di servizi di terze parti

Attacchi a livello fisico

- Attacchi Black-box
- Skimmer/modifiche del tastierino PIN
- Telecamere nascoste
- Esplosioni

Attacchi a livello di software

- Installazione di malware in locale/da remoto
- Sniffer di memoria/attacchi al sistema operativo
- Infezione/modifiche del middleware

Attacchi a livello di rete

- Vulnerabilità VPN
- Attacchi di forza bruta ai danni dell'RDP
- Exploit di rete che consentono vulnerabilità RCE
- Installazione da remoto

Sistemi integrati: vettori di attacco tipici

Sfide per la sicurezza dei dispositivi integrati

6 **Normativa.** Per via delle informazioni finanziarie e personali che possono elaborare, molti dispositivi integrati operano secondo normative che impongono un approccio particolarmente rigoroso alla sicurezza.

7 **Minacce interne.** In base ai dati Kaspersky, oltre il 50% di tutti gli attacchi andati a buon fine nei sistemi integrati comprende "attività di insider", ossia da parte di un dipendente o di un provider di servizi di terze parti.

8 **Diffusione di Linux.** Le piattaforme integrate stanno rapidamente guadagnando terreno, poiché offrono maggiore flessibilità e consentono l'utilizzo di una gamma più ampia di configurazioni. I cybercriminali ne stanno prendendo atto e la scelta di soluzioni di sicurezza moderne e specializzate è molto più limitata rispetto a quelle disponibili per Windows.

Caratteristiche principali

Protezione ottimale per qualsiasi scenario integrato:
Kaspersky Embedded Systems Security offre una protezione multilivello per garantire una sicurezza ottimale per i dispositivi con diversi livelli di potenza e scenari di implementazione. È incluso il supporto per le piattaforme basate su sistemi operativi diversi, come Windows e Linux

Protegge i sistemi nuovi e preesistenti
Kaspersky Embedded Systems Security è stato ottimizzato per integrarsi perfettamente con Windows XP, 7, 8, 10 e 11. Kaspersky continuerà a fornire il supporto per Windows XP nell'immediato futuro, offrendo ai clienti il tempo necessario per eseguire l'upgrade quando saranno pronti. Kaspersky Embedded Systems Security supporta anche le architetture più recenti con sistema operativo Windows o Linux.

Impatto ridotto sulle risorse, livelli elevati di protezione
Kaspersky Embedded Systems Security è stato creato per operare in modo efficace anche su hardware di fascia bassa.

Gli attacchi ai PoS e ai bancomat aumentano
In base ai dati delle ricerche di Kaspersky, il numero di attacchi ai danni di bancomat e sistemi PoS è cresciuto significativamente durante il 2022 e continua ad aumentare, con una crescita del 19% rispetto al 2020 e del 4% rispetto al 2021.

Funzionalità principali

Protezione avanzata del sistema (controlli di sicurezza). Queste tecnologie di protezione avanzata del sistema, che comprendono controlli per applicazioni, dispositivi e aggiornamento, consentono esclusivamente l'utilizzo di applicazioni, periferiche e origini di aggiornamento attendibili. Questo impedisce l'avvio e l'esecuzione di programmi non autorizzati, inclusi malware e app, che potrebbero essere utilizzati a scopi dannosi.

Anti-malware opt-in. Un livello di sicurezza opt-in rileva le minacce note, sconosciute e avanzate con una logica di rilevamento precisa, utilizzando intelligence sulle minacce locale o basata su cloud, nonché modelli euristici e di machine learning, in esecuzione on-premise o nel cloud.

Prevenzione exploit[1]. Impedisce lo sfruttamento delle vulnerabilità nelle app di terze parti e nei componenti di sistema in esecuzione di Windows, aiutando a contrastare gli attacchi più avanzati, inclusi quelli progettati per eludere il controllo delle applicazioni in modalità Default Deny e quelli che utilizzano tecniche senza file.

Protezione dalle minacce di rete. Previene eventuali intrusioni nel sistema operativo, proteggendo dalla scansione delle porte, dagli attacchi di forza bruta e dai cyberattacchi che sfruttano le vulnerabilità relative alla rete per compromettere il dispositivo preso di mira. In questo modo bloccherete uno dei principali vettori di attacco diretti ai sistemi integrati.

Monitoraggio dell'integrità e supporto per la conformità. Il monitoraggio dell'integrità dei file e dell'accesso al registro tiene traccia delle azioni eseguite su chiavi di registro, file e cartelle specifici e può bloccare eventuali modifiche indesiderate. Questo aiuta a rilevare non solo le intrusioni basate sul malware, ma anche le modifiche offline o con accesso diretto alle risorse critiche. Tali contromisure sono spesso specificamente consigliate nelle normative sulla protezione dei dati, pertanto abilitarle aiuta a mantenere la conformità.

Supporta i sistemi legacy e con scarse prestazioni. Supporta anche sistemi integrati a basso consumo in esecuzione su hardware obsoleto e sistemi operativi non supportati, fino a Windows XP SP2. Potete continuare a eseguire dispositivi obsoleti o desktop preesistenti in modo sicuro fino a quando non sarete pronti per l'upgrade.

Analisi dei log[1]. Eventuali violazioni della protezione vengono rilevate in base al monitoraggio e all'analisi dei registri eventi di Windows. L'applicazione avvisa l'amministratore quando rileva comportamenti anomali che possono indicare un tentativo di cyberattacco.

Gestione flessibile: on-premises o nel cloud. A seconda delle vostre esigenze aziendali, la sicurezza dei sistemi integrati aziendali può essere gestita da un server di gestione on-premise o da una console cloud SaaS Kaspersky Security Center, insieme ad altre soluzioni Kaspersky. Mentre la gestione on-premise è utile nei contesti con rigorosi requisiti di privacy, la console SaaS cloud gestita dal fornitore consente di risparmiare in termini di CAPEX e OPEX, permettendo un avvio rapido per processi di lavoro sicuri e meno problemi di manutenzione.

[1] Solo per i sistemi operativi Windows

Gestione del firewall. Il firewall del sistema operativo può essere configurato direttamente da Kaspersky Security Center, una console centralizzata che permette di gestire i firewall locali da un'unica console. Questo si rivela essenziale quando i sistemi integrati non sono nel dominio e le impostazioni del firewall di Windows/Linux non possono essere configurate a livello centrale.

Tolleranza per la scarsa connettività. Dal momento che molti tipi di dispositivi integrati sono spesso situati in remoto, una scarsa connettività (dovuta a una copertura cellulare inaffidabile o all'interferenza di fonti radio vicine e così via) non è insolita. Kaspersky Embedded System Security resta stabile anche con una larghezza di banda molto bassa, consentendo una protezione affidabile anche durante periodi prolungati di assenza di connettività.

Professional Services & Premium Support

La corretta manutenzione del ciclo di vita di una soluzione di sicurezza richiede impegno. Inoltre, a causa delle specifiche dei dispositivi integrati che li differenziano dai normali endpoint, mantenere la sicurezza dei sistemi integrati può essere particolarmente laborioso. Kaspersky Professional Services offre assistenza in ogni fase di questo ciclo di vita, dall'implementazione e l'aggiornamento alla configurazione e l'ottimizzazione delle prestazioni, fino alla migrazione a un hardware più recente. Inoltre, la nostra assistenza premium garantisce una risoluzione degli incidenti prioritaria da parte di esperti, con un Account Manager tecnico di grande esperienza.

Prodotti e servizi correlati

Kaspersky Threat Intelligence: una selezione versatile di servizi che offre una visione completa delle cyberminacce che prendono di mira la vostra organizzazione, combinando fonti di intelligence, feed di dati sulle minacce e ricerche interne, analizzate dai nostri esperti di sicurezza.

Valutazione della sicurezza dei sistemi di pagamento: l'analisi completa dei bancomat e dei dispositivi PoS offre un quadro completo dei livelli di sicurezza correnti, consentendovi di migliorare ulteriormente la sicurezza, di ottimizzarne la configurazione e colmare eventuali lacune.

Kaspersky Endpoint Security for Business: una piattaforma di protezione degli endpoint rinomata a livello mondiale che protegge endpoint, server, workstation e dispositivi mobili con le funzionalità di sicurezza più premiate e testate. Il tutto gestito da un'unica console.

Settori

- Servizi finanziari
- Trasporti e turismo (biglietterie)
- Retail
- Ristorazione e settore alberghiero
- Healthcare
- Enti governativi e attività non commerciali
- Intrattenimento

Dispositivi

- ATM
- Biglietterie automatiche
- Distributori di carburante
- Casse
- Punti vendita
- Apparecchiature mediche
- Endpoint legacy
- Slot machine e arcade machine

Novità sulle minacce informatiche: www.securelist.it
Tecnologie Kaspersky: kaspersky.com/technowiki
Novità sulla sicurezza IT:
www.kaspersky.it/blog/category/business/
Sicurezza IT per PMI:
www.kaspersky.it/small-to-medium-business-security
Sicurezza IT per l'azienda:
www.kaspersky.it/enterprise-security

Settori che utilizzano dispositivi integrati

www.kaspersky.it

We are proven. Siamo indipendenti. Siamo trasparenti. Siamo pronti a costruire un mondo sicuro, in cui le tecnologie migliorino le nostre vite. È per questo che lo proteggiamo, così che chiunque, in ogni luogo possa godere delle infinite opportunità che offre. Soluzioni di Cybersecurity Kaspersky, per un **futuro** più sicuro.

Altre informazioni sono disponibili alla pagina
kaspersky.it/about/transparency

**Proven.
Transparent.
Independent.**