Kaspersky Embedded Systems Security

kaspersky

Desafios de segurança embarcada

1. **Software obsoleto e vulnerável.** Ciclos de vida longos podem significar a execução de sistemas operacionais e aplicativos sem suporte, com vulnerabilidades não corrigidas apenas esperando para serem exploradas.
2. **Atualizações de segurança erráticas.** Mesmo quando ainda há suporte ao software, brechas nas versões de patching ainda podem ocorrer. Problemas relacionados à atualização de vários dispositivos dispersos geograficamente, tendo que colocá-los offline para serem atualizados (criando assim uma negação de serviço temporária) e a necessidade de testar atualizações antes de implantá-las podem contribuir para atrasos na aplicação de patches.
3. **Continuidade do processo.** Retirar certos tipos de dispositivos de serviço, mesmo que temporariamente – como equipamentos médicos, por exemplo – pode ser altamente problemático, aumentando ainda mais o intervalo de tempo de correção.
4. **Locais públicos.** Muitos dispositivos embarcados operam em espaços públicos abertos, o que aumenta muito o risco de violações. Defesas no nível de rede não conseguem proteger contra a contaminação física e direta do dispositivo.
5. **Natureza inerentemente arriscada.** Por estarem frequentemente associados diretamente a operações financeiras e processar informações pessoais confidenciais, os dispositivos embarcados são alvos especialmente atraentes para os cibercriminosos.

Segurança tudo em um desenvolvida para sistemas embarcados (e mais)

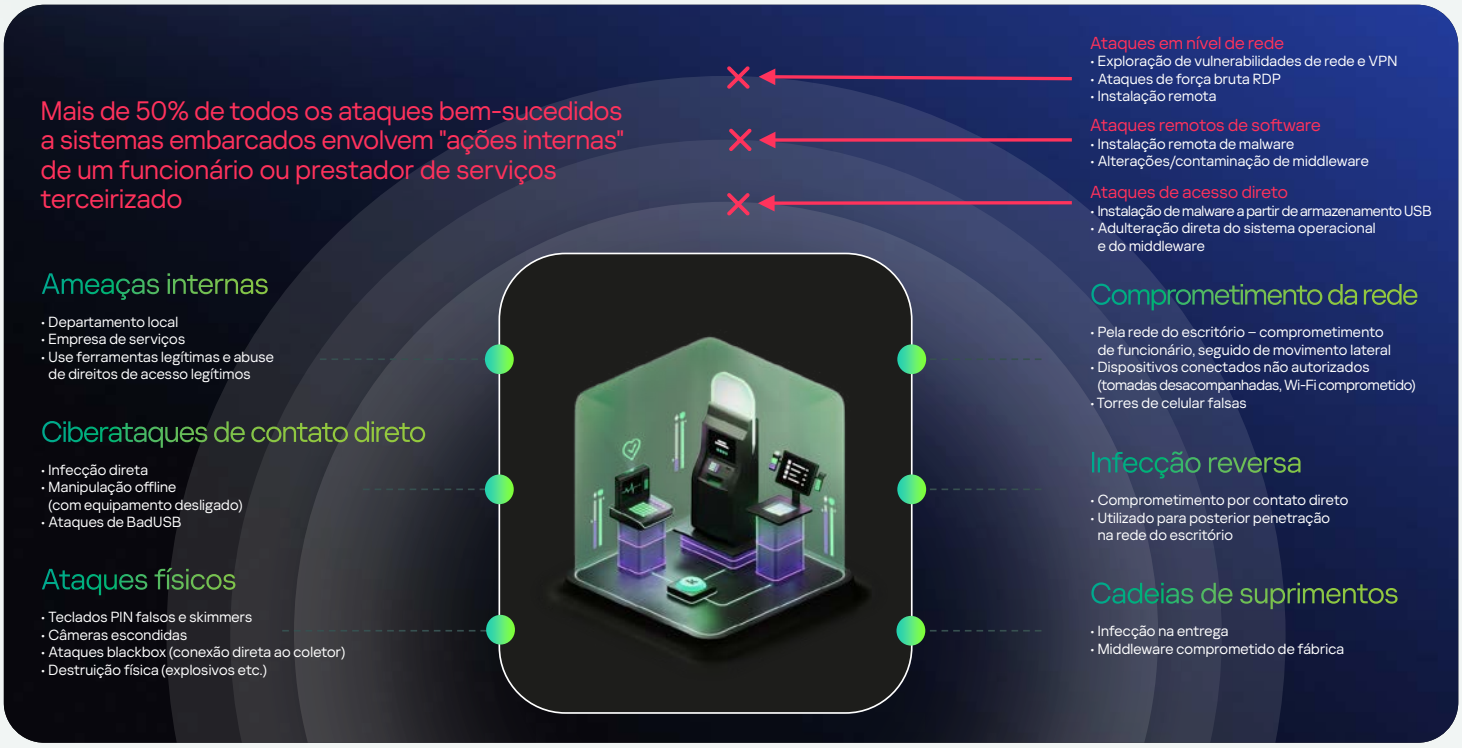
Os sistemas embarcados estão ao nosso redor e interagimos com eles todos os dias. Dependemos deles para tudo, de sistemas PoS e caixas eletrônicos a dispositivos médicos e bombas de combustível automatizadas. À medida que o mercado de sistemas embarcados cresce, os cibercriminosos estão acompanhando essa evolução, aprimorando suas táticas, técnicas e procedimentos para adequarem-se às especificidades desses sistemas generalizados.

Cenário de ameaças

Novos modelos de negócios criminosos, como Malware-as-a-Service, continuam a surgir, diminuindo as habilidades necessárias para outros potenciais invasores. Embora versões mais antigas do Windows tenham atingido o fim de seu suporte há muito tempo, elas ainda permanecem em operação (sendo o Windows XP o sistema operacional mais difundido em dispositivos embarcados). Milhões de dispositivos e PCs embarcados continuam a executar sistemas operacionais antigos e vulneráveis que, por algum motivo, não são atualizados. Isso acaba se tornando uma carta de boas vindas aos hackers.

Enquanto isso, sistemas embarcados baseados em Linux estão rapidamente ganhando popularidade, e os cibercriminosos estão percebendo, adaptando suas técnicas e criando instrumentos inteiramente novos para as especificidades dos sistemas embarcados em Linux. Superestimar a segurança inerente do Linux é perigoso – e embora os invasores tenham voltado sua atenção para dispositivos embarcados em Linux OS há relativamente pouco tempo, eles estão compensando o tempo perdido. O fato de que as ofertas atuais de cibersegurança para dispositivos embarcados em Linux sejam limitadas em comparação com o que está disponível para Windows não ajuda.

As empresas precisam ser mais inteligentes do que nunca para manter seus sistemas e dados seguros. Com poderosa Inteligência de Ameaças, detecção de malware opcional e prevenção de exploits, controles abrangentes de fortalecimento de sistema e gerenciamento flexível, o Kaspersky Embedded Systems Security é uma segurança tudo em um, projetada especificamente para sistemas embarcados (também conhecidos como sistemas embarcados). Ele fornece um nível exclusivo de proteção para sistemas antigos que não possuem mais suporte da maioria dos fornecedores de cibersegurança, e agora também oferece o mesmo nível de proteção para dispositivos mais modernos que executam Linux OS.



Sistemas embarcados: modelo de ameaças

Desafios de segurança embarcada

6 **Regulamentações rigorosas.** Devido às informações financeiras e de identificação pessoal que podem processar, muitos sistemas embarcados operam sob regulamentações que exigem uma abordagem particularmente diligente de segurança.

7 **Ameaças Internas.** De acordo com os dados da Kaspersky, mais de 50% de todos os ataques bem-sucedidos a sistemas embarcados envolvem "atividades internas" realizadas por um funcionário ou prestador de serviços terceirizado.

8 **Difusão do Linux.** Plataformas embarcadas estão ganhando popularidade rapidamente, oferecendo uma maior flexibilidade e permitindo o uso de uma variedade maior de configurações. Os cibercriminosos sabem disso, e a escolha de soluções de segurança modernas e especializadas é muito mais limitada em comparação ao que está disponível para o Windows.

Destaques

Proteção ideal para qualquer cenário embarcado:
O Kaspersky Embedded Systems Security oferece proteção multicamada, garantindo segurança de qualidade para dispositivos com diferentes níveis de desempenho e cenários de implementação. Isso inclui suporte para plataformas baseadas em diferentes sistemas operacionais, como Windows e Linux.

Proteção tanto para sistemas antigos, quanto novos
O Kaspersky Embedded Systems Security foi otimizado para ser executado com todos os recursos do Windows XP, 7, 8, 10, e 11. A Kaspersky continuará a oferecer suporte ao Windows XP no futuro, dando aos clientes tempo suficiente para atualizar quando estiverem prontos. O Kaspersky Embedded Systems Security também oferece suporte a arquiteturas mais recentes que executam o sistema operacional Windows ou Linux.

Poucos recursos, altos níveis de proteção
O Kaspersky Embedded Systems Security foi desenvolvido para funcionar de forma eficaz mesmo em hardware de baixo custo.

Parte de um ecossistema unificado
O Kaspersky Embedded Systems Security opera como parte integrante de uma família de soluções, gerenciada pelo mesmo console que outros produtos da Kaspersky e beneficiando-se de uma visibilidade centralizada e um fluxo de trabalho unificado.

Recursos principais

Fortalecimento do sistema (controles de segurança). Abrangendo controles de aplicativos, dispositivos e atualizações, essas tecnologias de fortalecimento do sistema só permitem o uso de aplicativos, periféricos de PCs e fontes de atualização confiáveis. Isso impede que programas não autorizados sejam iniciados e executados, incluindo malware e aplicativos que podem ser usados de forma maliciosa.

Opção de antimalware. Uma camada de segurança opcional detecta ameaças conhecidas, desconhecidas e avançadas com lógica de detecção precisa, usando inteligência de ameaças local ou baseada na nuvem, bem como heurística e modelos de aprendizado de máquina, com execução no local ou na nuvem. A tecnologia anticriptografia especializada garante que seus dispositivos não sofrerão os efeitos de ransomware.

Prevenção de exploits. Evita o exploit de vulnerabilidades na execução de componentes do sistema Windows e aplicativos de terceiros, ajudando a combater ataques mais avançados, incluindo aqueles projetados para evadir o controle de aplicativos do modo de Negação Padrão e aqueles que usam técnicas do tipo fileless.

Proteção contra ameaças de rede. Evita invasões do sistema operacional, protegendo contra varredura de portas, ataques de força bruta e ciberataques que exploram vulnerabilidades relacionadas à rede para comprometer o dispositivo de destino. Isso bloqueia um dos principais vetores de ataque direcionados a sistemas embarcados.

Monitoramento de integridade e suporte a conformidade. O monitoramento da integridade de arquivos e do acesso ao registro[1] rastreia ações executadas em chaves do registro, arquivos e pastas especificados e pode bloquear quaisquer alterações indesejadas. Isso ajuda a detectar não apenas invasões de malware, mas também acesso direto/modificações offline a recursos críticos. Essas contramedidas costumam ser especificamente recomendadas nas regulamentações de proteção de dados, portanto, ativá-las ajuda a manter a conformidade.

Oferece suporte a sistemas antigos e de baixo desempenho. A solução oferece suporte até mesmo a sistemas embarcados de baixo desempenho executados em hardware desatualizado, e sistemas operacionais sem suporte, até o Windows XP SP2. Você pode continuar executando dispositivos ou desktops antigos com segurança até que esteja pronto para atualizar.

Inspeção de Log[1]. Possíveis violações de proteção são detectadas com base no monitoramento e na inspeção dos logs de eventos do Windows. O aplicativo notifica o administrador quando detecta qualquer comportamento anormal que possa indicar uma tentativa de ciberataque.

Gerenciamento flexível – no local ou em nuvem. Dependendo das suas necessidades, a segurança dos seus sistemas embarcados corporativos pode ser gerenciada a partir de um servidor de gerenciamento local ou de um console Kaspersky Security Center SaaS na nuvem, junto com outras soluções da Kaspersky. Embora gerenciamento local seja útil onde um nível rigoroso de privacidade é necessário, o console SaaS na nuvem executado pelo fornecedor ajuda a economizar em CAPEX e OPEX, permitindo um início rápido para processos de trabalho seguros e com menos problemas de manutenção.

[1] somente para sistemas operacionais Windows

Gerenciamento de firewall. O firewall do sistema operacional pode ser configurado diretamente do Kaspersky Security Center, oferecendo a praticidade do gerenciamento de firewall local por meio de um único console unificado. Isso é essencial quando os sistemas embarcados não estão no domínio e as configurações de firewall do Windows/Linux não podem ser definidas centralmente. Para o sistema operacional Windows, está disponível um firewall proprietário em nível de aplicação, que reduz ainda mais a superfície de ataque por meio de um gerenciamento mais granular das conexões de rede dos aplicativos.

Tolerância à baixa conectividade. Como muitos tipos de dispositivos embarcados geralmente estão localizados remotamente, a conectividade ruim – como resultado de uma cobertura celular ruim, interferência de fontes de rádio próximas, etc. – não é incomum. O Kaspersky Embedded System Security permanece estável mesmo em banda larga muito baixa, mantendo proteção confiável mesmo durante períodos prolongados sem conectividade.

Integração de detecção e resposta gerenciadas: a solução se integra ao centro de operações de segurança da Kaspersky para monitoramento ininterrupto e resposta imediata. Isso possibilita a detecção e contenção precoces de ataques sofisticados a dispositivos embarcados, evitando perdas financeiras significativas para a empresa.

Serviços Profissionais e Suporte Premium

A manutenção adequada do ciclo de vida de uma solução de segurança exige esforço e, devido às especificidades dos dispositivos embarcados que os diferenciam dos endpoints comuns, manter a segurança dos sistemas embarcados pode ser especialmente trabalhoso. O Kaspersky Professional Services oferece assistência em todas as etapas deste ciclo de vida, desde a implantação e atualização, configuração e otimização de desempenho até a migração para hardwares mais recentes. E nosso suporte Premium garante a resolução prioritária e especializada de incidentes, com um account manager técnico dedicado, respaldado por experiência incomparável.

Produtos e serviços relacionados

Kaspersky Threat Intelligence: Uma seleção multi-funcional de serviços que oferece uma visão geral de ciberameaças direcionadas à sua organização, combinando fontes de inteligência, feeds de dados de ameaças e pesquisas internas, analisadas por nossos especialistas em segurança.

Payment Systems Security Assessment: Análise abrangente de seus caixas eletrônicos e dispositivos POS , fornecendo uma imagem clara de seus níveis de segurança atuais, permitindo aumentar ainda mais sua segurança, otimizar sua configuração e eliminar quaisquer falhas de segurança.

Linha de produtos Kaspersky Next: Combina proteção excepcional de endpoints e controles de segurança robustos com a transparência e a velocidade do EDR, e a visibilidade e as ferramentas poderosas de XDR, tudo isso em uma linha de produtos modular e flexível.

Setores

- Serviços financeiros
- Transporte e turismo (geração de bilhetes)
- Varejo
- Hospitalidade
- Serviços de saúde
- Governamental e não comercial
- Entretenimento

Dispositivos

- Caixas eletrônicos
- Máquinas de autoatendimento
- Bombas de combustível
- Caixas
- Pontos de venda
- Equipamento médico
- Endpoints de dispositivos antigos
- Máquinas caça-níqueis e fliperamas

Setores que usam dispositivos incorporados e sistemas embarcados

www.kaspersky.com.br

Somos comprovados. Somos independentes. Somos transparentes. Temos o compromisso de criar um mundo mais seguro, onde a tecnologia melhora nossas vidas. Por isso, nós a protegemos. Para que todos tenham acesso às infinitas oportunidades que ela proporciona. Traga o melhor da cibersegurança para um **futuro mais seguro**.

Saiba mais em kaspersky.com/about/transparency

Proven. Transparent. Independent.