Kaspersky® Embedded Systems Security

Une solution de sécurité tout-en-un conçue pour les systèmes embarqués

L'environnement des menaces évolue de façon exponentielle si bien que les processus commerciaux, les données confidentielles et les ressources financières sont de plus en plus menacés par des attaques « instantanées ». Pour atténuer les risques au sein de votre entreprise, vous devez être plus intelligent, mieux équipé et mieux informé que les cybercriminels.

Aujourd'hui, les systèmes embarqués sont partout : dans les distributeurs automatiques de billets de toutes sortes, les DAB, les bornes, les systèmes de point de vente, les dispositifs médicaux, etc. Les systèmes embarqués représentent une préoccupation particulière en matière de sécurité, en raison notamment de leur dispersion géographique, de la difficulté à les gérer et du manque de mises à jour. Ils doivent de plus être résistants et tolérants aux pannes car ils gèrent des opérations impliquant de l'argent réel et des informations d'identification de carte de crédit. Les appareils embarqués ne doivent pas uniquement être protégés contre les menaces : les cybercriminels et autres cyberpirates ne doivent pas non plus pouvoir s'en servir de point d'entrée pour pénétrer dans le réseau de l'entreprise.

La réglementation standard en matière de sécurité des appareils embarqués a tendance à ne couvrir que la sécurité basée sur des antivirus ou le renforcement du système, ce qui n'est pas suffisant. Une approche purement antivirus est d'une efficacité limitée contre les menaces rencontrées actuellement par les systèmes embarqués, comme cela a été amplement démontré lors des dernières attaques. Il est temps maintenant d'appliquer des technologies éprouvées telles que le contrôle des appareils et le blocage par défaut, associées si nécessaire à une protection antivirus supplémentaire pour les systèmes essentiels.

Points forts de la solution

Matériel de faible puissance

Kaspersky Embedded Systems Security a été développé spécifiquement pour fonctionner efficacement, même sur du matériel de faible puissance. Une conception efficace offre une sécurité puissante sans risque de surcharge des systèmes. Les prérequis débutent à seulement 256 Mo de RAM pour la famille Windows XP, avec environ 50 Mo d'espace disque nécessaire sur le disque dur pour l'installation en mode « blocage par défaut uniquement ».

Optimisation de Windows XP

La plupart des systèmes embarqués fonctionnent toujours avec les systèmes d'exploitation obsolètes de la famille Windows® XP. Kaspersky Embedded Systems Security a été optimisé pour être pleinement fonctionnel sur la plateforme Windows XP et les familles Windows 7, Windows 2009 et Windows 10.

La plupart des principaux fournisseurs de solutions de sécurité ne prennent plus en charge Windows XP. Kaspersky Embedded Systems Security s'engage à prendre intégralement en charge la famille Windows XP dans un avenir plus ou moins proche.

Blocage par défaut

Au cours des 10 dernières années, le nombre de programmes malveillants développés spécifiquement pour attaquer les systèmes embarqués (Tyupkin, Skimer, Carbanak et autres menaces dérivées) a augmenté. La plupart des solutions antivirus traditionnelles ne peuvent pas protéger totalement les équipements contre les menaces que représentent ces programmes malveillants ciblés avancés. Une solution classique de lutte contre les programmes malveillants reste inefficace contre d'autres types d'attaques basées sur des programmes non malveillants, notamment avec l'utilisation interne de middleware. Le mode de blocage par défaut permet qu'aucun fichier exécutable, pilote ou dll en dehors de ceux approuvés par l'administrateur, ne puisse s'exécuter.

Contrôle des périphériques

Le contrôle des périphériques de Kaspersky Lab permet de surveiller les appareils connectés ou tentant de se connecter physiquement aux systèmes. La prévention de l'accès par des appareils non autorisés élimine un point d'entrée utilisé régulièrement par les cybercriminels comme première étape d'une attaque par un programme malveillant.

Toutes les connexions d'appareils USB font l'objet d'une surveillance et d'une analyse. Toute utilisation USB inappropriée est traitée comme une attaque potentielle lors des processus d'investigation et de gestion des incidents.

Intégration SIEM

Kaspersky Embedded Systems Security peut désormais convertir les événements des journaux d'applications aux formats pris en charge par les serveurs Syslog. Tous les systèmes SIEM peuvent ainsi les reconnaître lors d'un transfert.

Protection de la mémoire

Kaspersky Embedded Systems Security protège les processus en mémoire contre l'exploitation de failles. Un agent de protection des processus chargé dynamiquement dans les processus protégés permet de surveiller leur intégrité et diminue les risques d'exploitation des vulnérabilités.

Administration centralisée

Les politiques de sécurité, les mises à jour des signatures, les analyses antivirus et la collecte des résultats sont gérées facilement par le biais d'une console de gestion centralisée unique : Kaspersky Security Center. Tous les agents d'un réseau local peuvent être gérés par l'intermédiaire d'une console locale, un atout de poids lorsque vous utilisez les réseaux segmentés et isolés caractéristiques des systèmes embarqués.

Maintenance et assistance

Nous intervenons 24 h sur 24, 7 jours sur 7 et 365 jours par an dans plus de 200 pays, à partir de nos 34 agences réparties dans le monde entier dans le cadre des offres d'assistance de notre contrat de maintenance et d'entretien (MSA).

Nos services professionnels restent à l'écoute pour vous garantir de profiter au maximum des avantages de votre installation de sécurité Kaspersky Lab.

Pour en savoir plus sur la protection de vos systèmes embarqués, rendez-vous sur www.kaspersky.fr/enterprise-security/embedded-systems

Gestion du pare-feu et des CD/DVD

En raison de la nature de certaines attaques de systèmes embarqués, il est indispensable de mettre en place une protection contre les activités malveillantes internes. Les systèmes embarqués utilisés en dehors du périmètre du domaine doivent toujours être protégés par une fonctionnalité de contrôle des appareils, gérée de manière centralisée, pour les lecteurs de CD/DVD internes et les supports de stockage USB. Un pare-feu est également nécessaire.

Surveillance de l'intégrité des fichiers

La surveillance de l'intégrité des fichiers permet de suivre les actions exécutées par les dossiers et fichiers spécifiques dans les limites données. Vous pouvez également configurer le suivi des modifications de fichiers pour qu'il ait lieu lorsque la surveillance est interrompue.

Audit des journaux

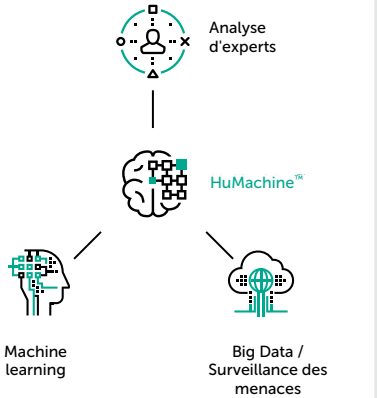
Kaspersky Embedded Systems Security surveille l'intégrité de l'environnement protégé en analysant les journaux d'événements de Windows. L'application prévient l'administrateur de tout comportement anormal détecté, signe d'une cyberattaque potentielle.

Pour cela, elle analyse les journaux d'événements de Windows et identifie les violations de sécurité en fonction des règles définies par l'utilisateur ou de la configuration de l'analyseur heuristique.

Antivirus et Kaspersky Security Network

L'antivirus est fourni comme module optionnel. Se contenter d'une approche classique contre les programmes malveillants n'est pas viable en raison des limitations du matériel bas de gamme et se révèle complètement inefficace dans ce contexte de menaces unique. Une fois Kaspersky Embedded Systems Security installée avec le contrôle des périphériques et le blocage par défaut, il n'est pas nécessaire d'ajouter un antivirus, sauf si vous souhaitez augmenter le niveau de sécurité.

Kaspersky Lab recommande également d'appliquer une sécurité intelligente grâce à la technologie Kaspersky Security Network afin de prévenir et d'atténuer les risques liés aux failles et de réduire le délai de réaction.



Solutions de sécurité Kaspersky Lab pour les entreprises : www.kaspersky.fr/enterprise-security
Actualités des cybermenaces : www.viruslist.fr
Actualités de la sécurité informatique : business.kaspersky.com

#truecybersecurity
#HuMachine

www.kaspersky.fr