MITIGUE RIESGOS DE SEGURIDAD CIBERNÉTICA CON ACTUALIZACIONES DE SOFTWARE PRE TESTEADAS

PROTEJA SUS SISTEMAS DE COMUNICACIONES DE MISIÓN CRÍTICA

ATAQUES CIBERNÉTICOS

75% EMPLEÓ VULNERABILIDADES QUE PODRÍAN HABER SIDO REPARADAS

BRECHAS EN SEGURIDAD

25% SON GENERADAS POR PERSONAS QUE PERTENECEN A LA ORGANIZACIÓN

73% SON PROVOCADAS POR ERRORES DE USUARIO O CONFIGURACIÓN INCORRECTA

Elevando el estándar en seguridad cibernética, CSIS, febrero de 2013

LOS SISTEMAS DE COMUNICACIÓN ESTÁN CADA VEZ MÁS EXPUESTOS A RIESGOS DE SEGURIDAD CIBERNÉTICA

Mientras la dependencia de sistemas basados en IP siga en aumento, el riesgo de intrusión y las amenazas a las que se ven expuestos los sistemas se volverán un desafío cada vez más complejo. Cuando los sistemas de comunicaciones de misión crítica se interconectan con otros sistemas basados en IP, quedan aún más expuestos a amenazas de seguridad cibernética en constante evolución.

CUMPLIMIENTO GARANTIZADO

Procedimientos de pre testeo y validación que garanticen la observancia de distintos mandatos de gobierno, normativas específicas de ciertos mercados y las mejores prácticas de la industria establecidas para optimizar las medidas de seguridad cibernética de los sistemas, entre as que se incluyen:

- Ley Federal de Administración de la Seguridad de la Información (FISMA)
- Proceso de Acreditación y Certificación de Aseguramiento de la Información del Departamento de Defensa (DIACAP)
- Política 4300A del Departamento de Seguridad Nacional
- Instituto Nacional de Normas y Tecnología: NIST 800-53
- Corporación Norteamericana de Confiabilidad Eléctrica (NERC)
- ISO 27001
- Normas de Seguridad de la Industria de Tarjetas de Pago (PCI)
- Otras directivas privadas

PRETESTEO DE ACTUALIZACIONES DE SOFTWARE QUE PROTEGE LA CONTINUIDAD OPERATIVA DEL SISTEMA

La sólida capacidad de parcheo (reparación) del sistema es una parte integral del programa global de seguridad cibernética de la organización. Las mejores prácticas de la industria sugieren que los parches de software deben aplicarse lo más pronto posible una vez lanzados por el proveedor. No obstante, es fundamental que toda actualización de software sea probada antes de su implementación en un sistema de misión crítica.

El Servicio de Actualización de Seguridad (SUS) de Motorola pre testea las últimas definiciones anti-malware y todos los parches de software aplicables en laboratorios de pruebas dedicados. Para las pruebas solo se identifican y seleccionan los parches aplicables requeridos para el sistema. Esto valida que no se introduzca ningún componente de software innecesario a través del proceso de parcheo. Una vez validadas como seguras para su implementación con la red de radio, las actualizaciones pueden ser implementadas para usted por Motorola, o pueden ser puestas a su disposición en el sitio de extranet seguro de Motorola.

Confíe en los expertos en seguridad certificados de Motorola para la identificación y la validación de las actualizaciones necesarias requeridas para mantenerse siempre al día en materia de seguridad cibernética. El Servicio de Actualización de Seguridad garantiza que se identifiquen, se validen y se apliquen los parches correctos de manera oportuna a fin de minimizar los riesgos de seguridad e incrementar la integridad operativa de su sistema de comunicaciones de misión crítica.

MINIMICE RIESGOS... Y COSTOS

Los Servicios de Actualización de Seguridad ofrecen:

Mayor disponibilidad de red
Reduzca las vulnerabilidades a las que están orientados los parches de seguridad e incremente el nivel de protección de la confidencialidad, la integridad y la disponibilidad de los sistemas de misión crítica.

Reduzca sus costos de mantenimiento
Minimice el tiempo de inactividad del sistema, lo cual deriva en la reducción de los costos asociados a las tareas de mantenimiento orientadas a poner el sistema nuevamente en funcionamiento.

Seguridad
Motorola asume la responsabilidad de verificar las actualizaciones de seguridad sin complicar innecesariamente a su personal.

Mayor aprovechamiento de recursos técnicos
Mantenga a su personal concentrado en sus tareas principales confiando en la experiencia y el soporte de Motorola para obtener el nivel de seguridad cibernética que necesita.

OPCIONES DE ENTREGA

Hay dos opciones disponibles para la implementación de actualizaciones de seguridad en su red de radio una vez que el software es pre testeado.

Descarga de cliente
Últimas actualizaciones de seguridad disponibles vía el sitio de extranet seguro de Motorola para que su equipo pueda descargarlas e instalarlas en su red de radio.

Entrega remota de SUS
El personal dedicado de Motorola puede instalar de manera remota las actualizaciones de seguridad en su red de radio. Las vulnerabilidades de software de otros proveedores son atendidas no bien se completa el proceso de validación de los parches recomendados. También proporcionaremos informes que sinteticen las actualizaciones para fines de revisión y reconocimiento por parte de su equipo.

Para más información sobre los Servicios de Seguridad, póngase en contacto con su representante local de Motorola o visite motorolasolutions.com/services

MOTOROLA