Libro blanco

Ciberseguridad de las plataformas RBX1 y MBX1

Índice

Ciberseguridad de las plataformas RBX1 y MBX1 3
Medidas a nivel de hardware y software 3
1 Criptoprocesador seguro 3
2 Arranque seguro y medido 4
3 Cifrado completo del disco 4
4 Actualizaciones de firmware autenticadas y cifradas 4
5 Acceso seguro con fines de asistencia y reparación 4
6 Ejecución de todos los procesos con los mínimos privilegios 4
7 Aislamiento efectivo del PC con Windows de la subestación 4
Medidas en el proceso de desarrollo de software 5
8 Arraigo de la ciberseguridad a nivel empresarial 5
9 Implementación segura 5
10 Pruebas de seguridad 5
11 Manejo de vulnerabilidades 5
Mediciones en el proceso de producción 6
12 Almacenamiento seguro de claves y certificados 6
13 Proceso de inicialización estricto 6
14 Servicio de dispositivo seguro 6
Cumplir los requisitos de seguridad más estrictos 6

Ciberseguridad de las plataformas RBX1 y MBX1

Las plataformas de hardware RBX1 y MBX1 se desarrollaron sobre la base de una metodología integrada de seguridad y satisfacen las exigencias más estrictas en materia de ciberseguridad e integridad. Se aplicaron medidas de seguridad adecuadas a nivel de hardware, software y procesos para reforzar el proceso de desarrollo, los propios productos y el proceso de producción frente a las ciberamenazas. Ambas plataformas y el proceso de desarrollo, el ciclo de vida de desarrollo de software seguro (SSDLC), están actualmente en proceso de certificación según la norma IEC 62443.

Medidas de ciberseguridad para los dispositivos RBX1 y MBX1

Proceso de desarrollo	Hardware y software	Proceso de producción
Arraigo de la ciberseguridad a nivel empresarial	Criptoprocesador seguro	Almacenamiento seguro de claves y certificados
Implementación segura	Arranque seguro y medido	Proceso de inicialización estricto
Pruebas de seguridad	Cifrado completo del disco	Servicio de dispositivo seguro
Manejo de vulnerabilidades	Actualizaciones autenticadas y cifradas	
Certificación IEC-62443 en curso	Acceso seguro con fines de asistencia y reparación	
	Principio de mínimos privilegios	
	Aislamiento efectivo del PC de la subestación	
	Certificación IEC-62443 en curso	

Este libro blanco estudia las medidas individuales de ciberseguridad introducidas en el diseño y desarrollo continuo de las plataformas RBX1 y MBX1.

Medidas a nivel de hardware y software

Para proteger los dispositivos RBX1 y MBX1 se utilizan componentes de hardware de última generación y un software integrado especialmente bastionado.

1 Criptoprocesador seguro

Ambos dispositivos incorporan un chip independiente de módulo de plataforma de confianza (TPM2.0) conforme a la norma ISO/IEC-11889. El chip genera y almacena certificados criptográficos de forma segura y da soporte el arranque seguro (véase la sección 2). Algunos certificados se guardan en este chip durante el proceso seguro de producción (véase la sección 13). El chip también genera claves únicas que se utilizan para cifrar los datos del dispositivo (véase la sección 3).

2 Arranque seguro y medido

Los dispositivos RBX1 y MBX1 utilizan una moderna interfaz UEFI (Unified Extensible Firmware Interface, interfaz unificada de firmware extensible) especialmente diseñada para OMICRON. La interfaz soporta el arranque seguro. Los procesos de arranque de los dispositivos se implementan mediante mecanismos de arranque seguro y medido. Esto evita que se ejecute software o código desconocido en un dispositivo. Cada paso del proceso de arranque comprueba la firma de la siguiente fase del proceso antes de que se ejecute dicha fase para garantizar que los RBX1 y MBX1 sólo cargan y ejecutan software que ha sido firmado por OMICRON. Además, la función de arranque seguro monitorea el hardware y software utilizado por los dispositivos. Si se detecta un cambio, todos los datos del dispositivo permanecen cifrados y el dispositivo no se inicia.

3 Cifrado completo del disco

Todos los datos críticos de los RBX1 y MBX1 están cifrados y sólo pueden ser descifrados por el dispositivo al que están asignados. La clave utilizada para cifrar los datos se genera en el criptochip de los RBX1 y MBX1 (véase la sección 1). Ni un tercero ni OMICRON pueden descifrar los datos, aunque se instale el disco duro en otro MBX1 o RBX1. Si los dispositivos detectan cualquier manipulación del contenido del disco duro durante el proceso de arranque, no se iniciarán. Si, por ejemplo, el código de cifrado de un dispositivo se ha visto comprometido, esto no tendrá ningún efecto sobre los datos del cliente en otro dispositivo. Sólo puede generarse un nuevo registro de claves mediante un restablecimiento de fábrica, que requiere acceso físico al dispositivo.

4 Actualizaciones de firmware autenticadas y cifradas

Las actualizaciones del firmware de los RBX1 y MBX1 están firmadas con un certificado de OMICRON (SHA512). Esto garantiza la autenticidad e integridad del archivo de actualización de firmware. Para evitar la ingeniería inversa, los archivos de actualización de firmware también se cifran mediante el mecanismo de cifrado AES-256-CBC. Las claves necesarias para el descifrado y la comprobación de la firma del archivo de actualización del firmware se guardan de forma segura en el chip del criptoprocesador (TPM 2.0).

5 Acceso seguro con fines de asistencia y reparación

El firmware y el hardware no contienen contraseñas por defecto ni otras puertas traseras. El acceso al RBX1 y al MBX1 con fines de mantenimiento sólo puede concederse temporalmente (la sesión se termina automáticamente tras un reinicio) y requiere un acceso físico pulsando el botón de reinicio situado en la parte trasera del dispositivo. Para conceder el acceso se utiliza un procedimiento de indagación-respuesta en lugar de una contraseña. El empleado de OMICRON tiene que resolver correctamente un problema criptográfico para obtener un acceso puntual al dispositivo. Este problema sólo puede resolverse utilizando la infraestructura de claves de OMICRON (véase la sección 12). Por lo tanto, no hay contraseñas predeterminadas ni claves generales que puedan caer en manos equivocadas.

6 Ejecución de todos los procesos con los mínimos privilegios

Todas las funciones críticas en los RBX1 y MBX1 se distribuyen en varios procesos. Cada proceso individual se ejecuta con el nivel más bajo de privilegios requerido para sus tareas según el principio de mínimos privilegios. Ningún proceso tiene privilegios de administrador o de raíz.

7 Aislamiento efectivo del PC con Windows de la subestación

Un PC con Windows (o varios PC) que ejecute StationScout, IEDScout o StationGuard y esté conectado al RBX1 o MBX1 sólo realiza funciones de visualización e interfaz de usuario. Todas las demás funciones son realizadas por el firmware seguro dentro del dispositivo. El RBX1/MBX1 no transfiere ningún dato entre los puertos de red de la subestación y los del controlador. En todas las aplicaciones de software compatibles, las comunicaciones con el dispositivo se autentican y cifran mediante TLS 1.3. StationScout y StationGuard sólo aceptan conexiones con dispositivos que puedan proporcionar el correspondiente certificado de seguridad. Ambos dispositivos también pueden aislar el PC de control y la red de la subestación a nivel de protocolo y sistema operativo. Por lo tanto, un PC con Windows potencialmente infectado permanece efectivamente aislado de la red de la subestación.

Medidas en el proceso de desarrollo de software

OMICRON ha creado un entorno de software seguro para el desarrollo de su software y firmware. Esto garantiza una norma constantemente exigente con respecto a la ciberseguridad en el proceso de desarrollo. Además de la capacitación en seguridad, la implementación segura y el control de calidad de la ciberseguridad, el proceso también abarca la detección y el manejo de posibles amenazas y vulnerabilidades asociadas a un producto específico. El ciclo de vida del desarrollo de software seguro (SSDLC) se basa en una serie de normas probadas, tal como la IEC 62443-4-1, la ISO 27000 y la NIST 800-30r1. El SSDLC garantiza que no se ignoren diversas medidas de seguridad durante el proceso de desarrollo. Describe cada fase del proceso, así como las medidas de seguridad estandarizadas y las mejores prácticas utilizadas.

8 Arraigo de la ciberseguridad a nivel empresarial

El SSDLC también garantiza que todos los desarrollos de software en OMICRON cumplan las normas de ciberseguridad correspondientes. El proceso comienza con un análisis del contexto de uso del producto y una definición de los requisitos de ciberseguridad, junto con un modelado a fondo de los riesgos. La implementación segura se basa en las normas establecidas y se verifica continuamente mediante pruebas de seguridad. Todos los pasos del proceso de desarrollo se documentan y se vuelven a comprobar al final para garantizar que se alcanza el nivel de seguridad requerido.

9 Implementación segura

Las comprobaciones de seguridad se llevan a cabo a lo largo de la fase de implementación para minimizar los problemas de seguridad. Para ello, se amplían las medidas preventivas, tal como el cumplimiento de las directrices para un código de programa seguro, mediante un examen minucioso del código en distintos ciclos de revisión. Entre los doce principios de seguridad que deben observarse actualmente figuran, por ejemplo, la reducción de la superficie de ataque minimizando el número de interfaces abiertas, el ya mencionado principio de los mínimos privilegios y la corrección de las vulnerabilidades identificadas en toda la base de código.

10 Pruebas de seguridad

Además de monitorear la implementación, el SSDLC también controla las pruebas de seguridad. Comprueba si se han cumplido los requisitos especificados y el nivel de ciberseguridad deseado. La práctica estándar a este respecto implica la comprobación del código del programa, las pruebas de seguridad dinámica y estática de la aplicación, el monitoreo de la seguridad de la aplicación y el análisis de la composición del software. Este último implica el escrutinio automatizado de los componentes y las vulnerabilidades de cada línea de código semanalmente. Las vulnerabilidades identificadas deben ser analizadas y corregidas por el equipo de desarrollo. En las plataformas RBX1 y MBX1, también se emplean pruebas de penetración para identificar cualquier vulnerabilidad de seguridad oculta.

11 Manejo de vulnerabilidades

En OMICRON nos tomamos muy en serio cualquier tipo de vulnerabilidad de seguridad que afecte a nuestros productos, por lo que agradecemos cualquier comentario que nos ayude a mejorar la seguridad de los mismos. Por ello, OMICRON ha introducido un flujo de trabajo sistemático para la presentación, gestión y divulgación de las vulnerabilidades de seguridad. Puede encontrar más información sobre el flujo de trabajo de gestión y divulgación de vulnerabilidades de seguridad de productos de OMICRON en https://www.omicronenergy.com/security.

Medidas en el proceso de producción

Además del proceso de desarrollo del software, también se han estudiado y adaptado los flujos de trabajo durante la producción del hardware RBX1 y MBX1 y su inicialización.

12 Almacenamiento seguro de claves y certificados

El manejo seguro de las claves y los certificados constituye la base de todas las medidas de seguridad restantes. El proceso de desarrollo seguro, así como los certificados y claves de nuestros productos, se generan y gestionan mediante una infraestructura segura. Esta infraestructura de claves se basa en los HSM (módulos de seguridad de hardware), que se encuentran en salas de servidores seguras. Los HSM impiden la extracción de las claves. Las claves privadas de OMICRON se generan en este hardware y no pueden extraerse, lo que significa que ni siquiera los empleados de OMICRON tienen acceso a ellas. Todas las claves y firmas asociadas, por ejemplo, de las actualizaciones de firmware, son generadas directamente por el hardware mediante un servicio especial. Sólo un número muy reducido de usuarios está autorizado a utilizar este servicio de firma, e incluso ellos sólo tienen acceso a los servicios esenciales para sus propias necesidades. La solución llega incluso a provocar la autodestrucción del HSM si se intenta forzar su apertura.

13 Proceso de inicialización estricto

Los dispositivos se inicializan en un paso de proceso ininterrumpido que sólo los empleados específicamente autorizados pueden llevar a cabo. Durante este proceso, los certificados criptográficos y las claves se guardan de forma segura en el chip TPM2.0. Los empleados correspondientes han recibido una capacitación específica sobre el tema de las amenazas a la seguridad y están muy concienciados sobre todos los aspectos de la seguridad de los datos en el lugar de trabajo y en su trato con personas externas.

14 Servicio de dispositivo seguro

El dispositivo se restablece antes de comenzar cualquier trabajo de reparación. Esto asegura que ya no contenga datos del cliente u otra información correspondiente a la seguridad. Una vez reparado el dispositivo, se repite el proceso de inicialización segura, al final del cual los técnicos de OMICRON pierden sus derechos de acceso. La renovación del acceso sólo será posible cuando el cliente vuelva a generar su archivo de indagación (véase la sección 5).

Cumplir los requisitos de seguridad más estrictos

Todas las medidas implementadas en las plataformas RBX1 y MBX1 y en las aplicaciones StationScout y StationGuard se reevalúan a intervalos predefinidos como parte de un proceso de mejora continua. Esto garantiza que todos los productos seguirán satisfaciendo los requisitos más estrictos en términos de ciberseguridad e integridad.

OMICRON trabaja con pasión en ideas pioneras para hacer que los sistemas eléctricos sean más seguros y confiables. Con nuestras soluciones innovadoras, hacemos frente a los retos presentes y futuros de nuestro sector. Estamos totalmente comprometidos con la asistencia a nuestros clientes: Nos tomamos en serio sus necesidades, les ofrecemos una excepcional asistencia en campo y compartimos nuestros conocimientos y experiencia.

El Grupo OMICRON desarrolla tecnologías innovadoras para todas las áreas de los sistemas eléctricos. El núcleo de sus actividades son las pruebas eléctricas de equipos de media y alta tensión, las pruebas de protección, las pruebas de subestaciones digitales y la ciberseguridad. Clientes de todo el mundo confían en nuestras soluciones de fácil uso y valoran su exactitud, rapidez y calidad.

Llevamos trabajando en el sector de la energía eléctrica desde 1984 y podemos presumir de tener muchos años de experiencia en el sector. Aproximadamente 900 empleados en 26 centros atienden a clientes de más de 160 países. Nuestro equipo de asistencia técnica está de guardia y disponible permanentemente.

Encontrará más información, un resumen general de la literatura disponible,
así como información detallada de contacto
con nuestras oficinas en todo el mundo
en nuestro sitio web.

www.omicronenergy.com