Whitepaper

Cyber Security der RBX1- und MBX1-Plattformen

Inhalt

Cyber Security der RBX1- und MBX1-Plattformen

Die beiden Hardwareplattformen RBX1 und MBX1 wurden gemeinsam auf Basis eines holistischen Security-Ansatzes entwickelt und genügen höchsten Ansprüchen an Cyber Security und Integrität. Entsprechende Sicherheitsmaßnahmen werden auf Hardware-, Software- und Prozessebene gesetzt, um den Entwicklungsprozess, die Produkte selbst und den Produktionsprozess gegenüber Cybergefahren zu härten. Beide Plattformen als auch der Entwicklungsprozess, Secure Software Development Life Cycle (SSDLC), durchlaufen derzeit die Zertifizierung nach IEC 62443.

Maßnahmen für die Cyber Security von RBX1 und MBX1

Entwicklungsprozess	Hardware & Software	Produktionsprozess
Verankerung von Cyber Security auf Unternehmensebene	Sicherer Krypto-Prozessor	Sichere Verwahrung von Schlüsseln und Zertifikaten
Sichere Implementierung	Secure & Measured Boot	Strikter Einrichtungsprozess
Sicherheitstests	Vollständige Festplatten-verschlüsselung	Sicherer Geräte-Service
Behandlung von Schwachstellen	Authentifizierte und verschlüsselte Updates	
IEC-62443-Zertifizierung im Gange	Sicherer Support- und Reparaturzugriff	
	Prinzip der „Least Privileges“	
	Effektive Isolierung des PCs von der Anlage	
	IEC-62443-Zertifizierung im Gange	

Der folgende Artikel beleuchtet die einzelnen Cyber-Security-Maßnahmen, die im Design und der Weiterentwicklung von RBX1 und MBX1 gesetzt werden.

Maßnahmen auf Hard- und Software-Ebene

Zur Absicherung der beiden Geräte RBX1 und MBX1 kommen modernste Hardwarekomponenten und eine speziell gehärtete Embedded-Software zum Einsatz.

1 Sicherer Krypto-Prozessor

Beide Geräte sind mit einem separaten und ISO/IEC-11889-konformen Trusted-Platform-Module(TPM2.0)-Chip ausgestattet, der kryptografische Zertifikate sicher erzeugen und speichern kann und Secure Boot unterstützt (siehe Abschnitt 2). Bestimmte Zertifikate werden während des sicheren Produktionsprozesses auf diesem Chip gespeichert (siehe Abschnitt 13). Dieser Chip generiert auch jeweils einzigartige Schlüssel, mit denen die Daten auf dem Gerät verschlüsselt werden (siehe Abschnitt 3).

2 Secure Boot und Measured Boot

RBX1 und MBX1 verwenden ein modernes, speziell für OMICRON angefertigtes UEFI (Unified Extensible Firmrware Interface), das Secure Boot unterstützt. Der Bootprozess der Geräte wird mit Hilfe von den Secure- und Measured-Boot-Mechanismen implementiert. Dieser Prozess verhindert, dass unbekannte Software oder Code auf dem Gerät ausgeführt wird. Jeder Schritt im Bootprozess überprüft die Signatur der nächsten Phase des Prozesses, bevor diese ausgeführt wird. Dadurch wird sichergestellt, dass RBX1 und MBX1 nur Software lädt und ausführt, die von OMICRON signiert wurde. Darüber hinaus überwacht die sichere Boot-Funktion die Hard- und Software der Geräte. Wird eine Änderung erkannt, bleiben die Daten auf dem Gerät verschlüsselt und es startet nicht.

3 Vollständige Festplattenverschlüsselung

Alle kritischen Daten auf der RBX1 und MBX1 sind verschlüsselt und können nur von genau dem Gerät entschlüsselt werden, dem sie zugeordnet sind. Die für die Verschlüsselung der Daten verwendeten Schlüssel werden im Kryptochip der RBX1 und MBX1 erzeugt (siehe Abschnitt 1). Weder Dritte noch OMICRON können die Daten entschlüsseln, selbst wenn die Festplatte in ein anderes MBX1 oder RBX1 eingebaut wird. Eine Manipulation der Festplatteninhalte erkennen die Geräte während des Bootvorgangs und verhindern den Start. Würden beispielsweise die Verschlüsselungscodes eines Geräts kompromittiert, bleiben Kundendaten auf einem anderen Gerät davon unbeeinflusst. Die Generierung eines neuen Schlüsselsatzes ist nur durch einen Factory-Reset möglich. Hierzu ist der physische Zugriff auf das Gerät erforderlich.

4 Authentifizierte und verschlüsselte Firmware-Updates

Firmware-Upgrades für RBX1 und MBX1 werden mit einem OMICRON-Zertifikat signiert (SHA512). Dies gewährleistet die Authentizität und Integrität der Firmware-Update-Datei. Zusätzlich werden die Firmware-Update-Dateien mit dem aes-256-cbc-Verschlüsselungsmechanismus verschlüsselt, um Reverse Engineering zu verhindern. Die Schlüssel zur Entschlüsselung und Signaturprüfung der Firmware-Update-Datei sind sicher auf dem Krypto-Prozessor(TPM 2.0)-Chip gespeichert.

5 Sicherer Support- und Reparaturzugriff

Firmware und Hardware enthalten weder Standardpasswörter noch andere Backdoors. Der Wartungszugriff auf die RBX1 und MBX1 kann nur vorübergehend gewährt werden (die Sitzung wird bei einem Neustart automatisch geschlossen) und ist nur mit physischem Zugriff durch Drücken des Reset-Knopfes auf der Rückseite möglich. Der Zugriff erfolgt nicht passwortbasiert, sondern über ein Challenge-Response-Verfahren. Dabei muss der der/die OMICRON-MitarbeiterIn eine kryptografische Aufgabe lösen, um einmaligen Zugriff auf das Gerät zu erhalten. Diese Aufgabe kann nur mittels der OMICRON-Schlüsselinfrastruktur (siehe Abschnitt 12) gelöst werden. Dadurch gibt es kein Standardpasswort oder Generalschlüssel, die in falsche Hände geraten könnte.

6 Ausführung aller Prozesse mit den geringsten Berechtigungen

Alle kritischen Funktionen auf der RBX1 und MBX1 sind in verschiedene Prozesse unterteilt. Jeder einzelne Prozess läuft mit den geringsten für seine Aufgabe erforderlichen Berechtigungen, nach dem Prinzip der „Least Privileges“. Kein Prozess hat Administrator- oder Root-Rechte.

7 Effektive Isolierung des Windows-PCs von der Anlage

Ein Windows-PC (oder auch mehrere), der mit StationScout, IEDScout, oder StationGuard arbeitet und an die RBX1 oder MBX1 angeschlossen ist, führt nur Funktionen für die Visualisierung und Benutzeroberfläche aus. Alle anderen Funktionen werden in der sicheren Firmware innerhalb des Geräts ausgeführt. Das RBX1/MBX1 überträgt keine Daten zwischen den Netzwerk-Ports für die Schaltanlage und denen für die Steuerung. Bei allen kompatiblen Softwarelösungen wird die Kommunikation mit dem Gerät mit TLS 1.3 authentifiziert und verschlüsselt. Sowohl StationScout als auch StationGuard akzeptieren dabei nur Verbindungen zu Geräten, die das entsprechende Sicherheitszertifikat bereitstellen. Beide Geräte verfügen zudem über eine Trennung auf Protokoll- und Betriebssystemebene zwischen dem steuernden PC und dem Anlagennetzwerk. Ein potentiell infizierter Windows-PC bleibt dadurch effektiv vom Schaltanlagennetzwerk isoliert.

Maßnahmen im Software-Entwicklungsprozess

Bei der Entwicklung von Software oder Firmware hat OMICRON einen sicheren Softwareentwicklungsprozess etabliert, um einen durchgehend hohen Standard in Bezug auf Cyber Security in der Entwicklung zu gewährleisten. Neben Security-Schulungen, der sicheren Implementierung und der Cyber-Security-Qualitätssicherung befasst sich der Prozess auch mit der Erfassung und Behandlung von potenziellen Bedrohungen und Schwachstellen, die für ein bestimmtes Produkt gelten. Der Secure Software Development Life Cycle (SSDLC) basiert auf mehreren bewährten Standards, wie IEC 62443-4-1, ISO 27000 und NIST 800-30r1. Der SSDLC stellt sicher, dass diverse Sicherheitsmaßnahmen in der Entwicklung berücksichtigt werden. Er beschreibt jede Phase des Entwicklungsprozesses sowie die standardisierten Sicherheitsmaßnahmen und Best Practices, die dabei zum Einsatz kommen.

8 Verankerung von Cyber Security auf Unternehmensebene

Der SSDLC gewährleistet, dass jede Softwareentwicklung bei OMICRON entsprechenden Cyber-Security-Standards folgt. Am Beginn des Prozesses steht die Analyse des Nutzungskontextes des Produktes und die Definition der Anforderungen an die Cyber Security, sowie eine umfassende Gefahrenmodellierung. Die sichere Implementierung orientiert sich an etablierten Standards und wird mittels Sicherheitstests laufend verifiziert. Sämtliche Entwicklungsschritte werden dokumentiert und abschließend kontrolliert, damit das angestrebte Sicherheitsniveau erreicht wird.

9 Sichere Implementierung

Während der gesamten Implementierungsphase kommen Sicherheitskontrollen zum Einsatz, um Sicherheitsmängel zu minimieren. Dafür werden vorbeugende Maßnahmen, wie die Berücksichtigung von Richtlinien für sicheren Programmcode, durch die genaue Überprüfung des Codes in getrennten Review-Schleifen ergänzt. Zu den derzeit zwölf Sicherheitsprinzipien, die berücksichtigt werden müssen, gehören beispielsweise die Reduktion der Angriffsfläche durch Minimierung der offenen Schnittstellen, das bereits erwähnte Prinzip der geringsten Privilegien und die Behebung von identifizierten Schwachstellen über die gesamte Codebasis hinweg.

10 Sicherheitstests

Wie die Implementierung sind auch die Sicherheitstests im SSDLC geregelt. Dabei wird überprüft, ob die definierten Anforderungen und das angestrebte Niveau an Cyber Security erreicht wurde. Hierfür werden standardmäßig Überprüfungen des Programmcodes, dynamische (DAST, dynamic application security testing) und statische (SAST, static application security testing) Überprüfungen der Anwendungssicherheit sowie die Analyse der Softwarezusammensetzung (SCA, software composition analysis) durchgeführt. Bei letzterer wird wöchentlich die gesamte Codebasis auf ihre Komponenten und deren Schwachstellen automatisiert durchleuchtet. Identifizierte Schwachstellen müssen im Anschluss vom Entwicklungsteam analysiert und behandelt werden. Bei den Plattformen RBX1 und MBX1 wird noch zusätzlich mit Penetrationstests gearbeitet, um versteckte Sicherheitslücken zu identifizieren.

11 Behandlung von Schwachstellen

Bei OMICRON wird jede Art von Schwachstelle (Security Vulnerability), die unsere Produkte betrifft, sehr ernst genommen, weshalb wir jeden Hinweis zur Verbesserung der Produktsicherheit sehr schätzen. Aus diesem Grund hat OMICRON einen systematischen Ansatz für die Einreichung, die Behandlung und die Offenlegung von Security-Schwachstellen eingeführt. Weitere Details zum OMICRON Product Security Vulnerability Handling and Disclosure Workflow finden Sie unter https://www.omicronenergy.com/security.

Maßnahmen im Produktionsprozess

Neben dem Softwareentwicklungsprozess wurden für RBX1 und MBX1 auch die Abläufe während der Produktion der Hardware und deren Einrichtung durchleuchtet und entsprechend angepasst.

12 Sichere Verwahrung von Schlüsseln und Zertifikaten

Der sichere Umgang mit Schlüsseln und Zertifikaten ist das Rückgrat aller anderen Sicherheitsmaßnahmen. Der sichere Entwicklungsprozess und die Zertifikate und Schlüssel in unseren Produkten werden über eine sichere Infrastruktur erzeugt und verwaltet. Diese Schlüssel-Infrastruktur basiert auf HSMs (Hardware Security Modules), die sich in gesicherten Serverräumen befinden. Diese HSMs verhindern, dass Schlüssel extrahiert werden können. OMICRON‘s private Schlüssel wurden in dieser Hardware erzeugt und können nicht extrahiert werden. Somit hatte auch kein OMICRON-Mitarbeiter jemals Zugriff auf die privaten Schlüssel. Alle abhängigen Schlüssel oder Signaturen, z.B. von Firmware-Updates werden direkt von der Hardware über einen speziellen Dienst erzeugt. Nur eine sehr begrenzte Anzahl von Benutzern hat die Berechtigung, diesen Signierdienst zu nutzen, und sie haben nur Zugriff auf genau die Dienste, die sie unbedingt benötigen. Die Lösung geht dabei soweit, dass sich das HSM selbst zerstört, wenn versucht wird, es mechanisch zu öffnen.

13 Strikter Einrichtungsprozess

Die Einrichtung der Geräte wird in einem ununterbrochenen Prozessschritt erledigt und kann nur von einzelnen autorisierten Mitarbeitern durchgeführt werden. Während dieses Prozesses werden die kryptografischen Zertifikate und die Schlüssel sicher auf dem TPM2.0-Chip gespeichert. Die damit betrauten Mitarbeiter sind spezifisch zum Thema Sicherheitsbedrohungen geschult und haben ein geschärftes Bewusstsein in den Bereichen Datensicherheit am Arbeitsplatz und im Umgang mit externen Personen.

14 Sicherer Geräte-Service

Bevor ein Gerät den Reparaturprozess durchläuft, wird dieses zuerst zurückgesetzt. Damit wird sichergestellt, dass sich keine Kundendaten oder sicherheitsrelevante Informationen mehr darauf befinden. Nach der Gerätereparatur wird der sichere Einrichtungsprozess erneut durchlaufen, an dessen Ende auch die OMICRON-Techniker den Zugriff wieder verlieren. Ein erneuter Zugriff ist wiederum nur möglich, wenn der Kunde seine Challenge-Datei ein weiteres Mal teilt (siehe Abschnitt 5).

Erfüllung höchster Sicherheitsansprüche

Sämtliche Maßnahmen, die bei den beiden Plattformen RBX1 und MBX1 sowie den Softwarelösungen StationScout und StationGuard zum Einsatz kommen, werden nach definierten Intervallen neu evaluiert und in einem kontinuierlichen Prozess verbessert. Damit wird sichergestellt, dass alle Produkte auch in Zukunft höchste Ansprüche in Bezug auf Cyber Security und Integrität erfüllen.

OMICRON arbeitet mit Leidenschaft an wegweisenden Ideen, um Energiesysteme sicherer und zuverlässiger zu machen. Mit unseren neuartigen Lösungen stellen wir uns den aktuellen und zukünftigen Herausforderungen unserer Branche. Wir zeigen vollen Einsatz bei der Unterstützung unserer Kund*innen: Wir gehen auf ihre Bedürfnisse ein, bieten ihnen hervorragenden Vor-Ort-Support und teilen unsere Expertise und unsere Erfahrungen mit ihnen.

In der OMICRON-Gruppe entwickeln wir innovative Technologien für alle Bereiche elektrischer Energiesysteme. Im Fokus stehen elektrische Prüfungen an Mittel- und Hochspannungsbetriebsmitteln, Schutzprüfungen, Prüfungen digitaler Schaltanlagen und Cyber Security. Kund*innen in aller Welt vertrauen auf unsere einfach zu bedienenden Lösungen und schätzen deren Genauigkeit, Schnelligkeit und Qualität.

Wir sind seit 1984 in der elektrischen Energietechnik tätig und verfügen über fundierte, langjährige Erfahrung in der Branche. Rund 900 Mitarbeiter*innen an 26 Standorten unterstützen unsere Kund*innen in mehr als 160 Ländern und unser technischer Support kümmert sich 24 Stunden am Tag, 7 Tage die Woche um sie.

Mehr Informationen, eine Übersicht der verfügbaren Literatur und detaillierte Kontaktinformationen unserer weltweiten Niederlassungen finden Sie auf unserer Website.

www.omicronenergy.com