HENSOLDT Cyber

Pressemitteilung

Taufkirchen, 29.04.2020

Sichere IT ist wichtig – nicht nur in Krisenzeiten

In Krisenzeiten sind IT, vernetzte Anlagen in der Industrie und das IoT durch verstärkte Cyberangriffe besonders gefährdet. HENSOLDT Cyber stellt mit dem Betriebssystem TRENTOS und dem RISC-V-Prozessor MiG-V Lösungen „Made in Germany" bereit, die Unternehmen dabei helfen, den Herausforderungen zu begegnen.

Die rasche Ausbreitung von Sars-CoV-2 führte in vielen Unternehmen zu einem eiligen Aufbruch ganzer Abteilungen ins Homeoffice. Und das bringt Sicherheitsprobleme mit sich: Statt über gesicherte interne Firmennetzwerke wird über das offene Internet kommuniziert. Viele Übertragungswege sind ungesichert, nicht auf die notwendige Bandbreite ausgelegt und Server überlastet. Verschärft wird dies häufig durch die Verwendung privater Geräte, deren Betriebssysteme, Anwenderprogramme und Sicherheitssoftware oftmals nicht auf den aktuellen Stand sind oder von Haus aus Fehler aufweisen.

So warnen Dienstleister wie Sophos vor „Myriaden von Bedrohungen" durch Trittbrettfahrer des Virus, und das Bundesamt für Sicherheit in der Informationstechnologie sieht eine „exponentielle Zunahme von Registrierungen von Webseiten mit Sars-CoV-2- oder COVID-19-Bezug", die für die Verbreitung von Schadsoftware genutzt werden. Dass Cyberkriminelle bereits aktiv sind, bezeugen betrügerische E-Mails und originalgetreu replizierten Seiten zur Beantragung von Soforthilfen, um Daten abzugreifen.

Betroffen sind aber nicht nur die klassische Informationstechnologie (IT) oder die Geräte im Homeoffice, sondern ebenfalls die operative Technologie (OT), also vernetzte Produktionsanlagen und Maschinen in der Industrie, ebenso wie das Internet der Dinge (IoT) mit ihren ungezählten Embedded-Systemen. Auch diese Domänen sind gefährdet, da hier Softwareaktualisierungen oftmals nicht verfügbar sind und die von den Herstellern vorgegebenen Standardpasswörter häufig unverändert weiterbenutzt werden. Dabei können gerade in produktionsnahen Bereichen durch Angriffe schnell materielle und immaterielle Schäden in Millionenhöhe entstehen.

Unternehmen müssen also ihre IT-Sicherheit neu überdenken. Nicht nur, um auf die aktuelle Gefahrenlage zu reagieren, sondern auch, um sich für die Zukunft zu wappnen.

Um Anlagen und Geräte vor virtuellen Angriffen zu schützen, stellt das in Taufkirchen bei München ansässige Start-up HENSOLDT Cyber zwei Neuentwicklungen „Made in Germany" bereit. Diese folgen dem Ansatz „Sichere IT statt IT-Sicherheit" für einen besseren Schutz im Cyberspace.

Dabei handelt es sich zum einen um TRENTOS, ein hochsicheres Betriebssystem, das auf einem sicheren und sehr kleinen Mikrokernel aufbaut, bei dem erstmalig die Sicherheit der kritischen

Komponenten durchgängig mathematisch formal verifiziert ist. Dieser Mikrokernel ist der von akademischen Partnern in Sydney entwickelte seL4-Mikrokernel und wurde für die offene Befehlssatzarchitektur RISC-V angepasst. Eines der wichtigsten Sicherheitsprinzipien dieses Kerns ist die strikte Trennung der einzelnen Software Komponenten, welche auf diesem betrieben werden. Diese können nur dann untereinander interagieren, wenn sie speziell dafür konfiguriert sind. Der Administrator behält damit die volle Kontrolle über sein IoT-Netzwerk.

Das Design von TRENTOS bietet Sicherheitseigenschaften basierend auf bewiesenen Integritätseigenschaften. Dazu wurde der Mikrokernel zunächst mathematisch formuliert und anschließend mittels eines halbautomatischen Theorem-Beweises die Korrektheit belegt. Dies stellt sicher, dass eventuelle Angreifer nicht über eine gegebenenfalls kompromittierte Komponente hinaus weiter ins System vordringen können. Das Betriebssystem ist in zwei Varianten verfügbar: TRENTOS-M für den Einsatz in Embedded-Systemen mit höchstem Schutzbedarf, sowie TRENTOS-G für den Einsatz in komplexeren Systemen. TRENTOS-M bietet dabei speziell auf Sicherheit ausgelegte Betriebssystemservices wie sicheres Booten und sichere Updates, Zertifikatsparser, Schlüsselspeicher auch einen Konfigurationsserver sowie ein TLS- und ein Kryptomodul.

Als zweiten Baustein für eine sichere IT bietet HENSOLDT Cyber mit dem MiG-V einen universellen, logisch verschlüsselten Prozessor „Made in Germany“ an, der auf Hochsicherheitsanwendungen ausgerichtet ist. Die logische Verschlüsselung verhindert das nachträgliche Einfügen von Hardware-Trojanern in die Architektur während des Fertigungsprozesses und gibt HENSOLDT Cyber die volle Kontrolle über die Design- und Produktionskette. Die zentrale Recheneinheit (CPU) basiert auf der quelloffenen Befehlssatzarchitektur RISC-V und wurde als RV64IMAC mit 64-Bit Integer-CPU und den Erweiterungen für Integer-Multiplikation/Division (M), atomische Speicheroperationen (A) und verkürzte Befehle (C) implementiert.

Zusammen mit dem im internen ROM-Speicher des Prozessors abgelegten TRENTOS-Mikrokernel schafft der MiG-V als Allzweck-Prozessor eine hochsichere Lösung für Anwendungen im Internet der Dinge und der operativen Technologie. Als Peripherie verfügt der MiG-V über ein 1 MByte großes internes SRAM, einen 2 MByte großen Flash-Speicher und einen bis zu 100 MHz schnellen SDRAM-Controller. Zur Kommunikation mit externen Bauelementen sind zwei 10/100 MBit/s Ethernet-MAC-Controller, ein QSPI- und drei SPI-Controller mit bis zu 30 MHz und ein SPI-Slave-Interface mit bis zu 40 MHz sowie drei UART-Controller und ein I2C-Controller vorhanden. Der Chip wird mit einer Versorgungsspannung von 3,3 V betrieben.

Die von HENSOLDT Cyber entwickelten Lösungen sind optimal auf die Sicherheitsbedürfnisse von Unternehmen zugeschnitten: „Herkömmliche IT- und OT-Lösungen sind von Natur aus anfällig, und Standard-Add-on-Sicherheitsprodukte behandeln eher Symptome, als dass sie die zugrunde liegenden Probleme angehen und erreichen daher keine wirkliche Sicherheit“, sagt Sascha Kegreiß, der CTO von HENSOLDT Cyber. „Unser Ansatz zur Cybersicherheit ist radikal anders: Sichere IT statt IT-Sicherheit. Und das ‚Made in Germany.‘ Wir bauen Systeme, die von Grund auf sicher sind, indem wir innovativen physischen Schutz mit mathematischen Beweisen für die Korrektheit von Software

kombinieren, um echte Vertrauenswürdigkeit zu erreichen“, so Kegreiß, der auch Mitglied im Governing Board der neu gegründeten sel4-Foundation ist, weiter.

HENSOLDT Cyber ist durch die Zusammenarbeit mit akademischen Partnern gut für die Lösung von Problemen im Bereich der Cybersicherheit aufgestellt. Gemeinsam mit führenden Chief Scientists werden zukunftsweisende Lösungen „Made in Germany“ erarbeitet. So unterstützt Professor Dr. Rainer Leupers von der RWTH Aachen University die Hardwareentwicklung, Professor Dr. Gernot Heiser von der University of New South Wales den Bereich Software und Dr. Sandro Gaycken, Direktor des Digital Society Institutes in Berlin, die Architekturentwicklung. Daneben hat HENSOLDT Cyber auch ein Team aus mehr als 40 Spezialisten aufgebaut, die in den Bereichen Soft- und Hardware, Kryptographie, Verifikation sowie im Penetration-Testing tätig sind. Damit steht eine geballte Expertenkompetenz für Sicherheitslösungen „Made in Germany“ zur Verfügung.

Zusätzlich zu den vorgestellten Lösungen bietet HENSOLDT Cyber auch Beratungsleistungen und entwicklungsbegleitende Aktivitäten an. Darunter fallen beispielsweise die Risikobewertung vorhandener Produkte und die detaillierte Analyse möglicher Schwachstellen des Designs und der eingesetzten Komponenten. Hier stellt HENSOLDT Cyber neben seinen Kompetenzen in Soft- und Hardware auch sein Know-how in Sachen Kryptographie bereit.

Über HENSOLDT Cyber

Die 2017 gegründete HENSOLDT Cyber GmbH ist ein deutsches Unternehmen mit Sitz in Taufkirchen bei München, das eingebettete Produkte der Informationstechnologie entwickelt, welche den höchsten Sicherheitsanforderungen entsprechen. Diese integrieren ein hochsicheres Betriebssystem mit gehärteter Hardware und schaffen so für den globalen IT-Markt eine sichere IT anstatt IT-Sicherheit. Das Unternehmen kombiniert die über 50-jährige Erfahrung der HENSOLDT Gruppe in der Verteidigungs- und Sicherheitselektronik mit Weltklasse-Expertise in der Hard- und Software-Entwicklung. Aktuell beschäftig HENSOLDT Cyber um die 40 Mitarbeiter an verschiedenen Standorten.

Weitere Informationen zum Unternehmen finden Sie auf unserer Website www.hensoldt-cyber.com

Bildunterschrift
HENSOLDT Cyber Lösungen für die Industrie 4.0

Bildunterschrift
Sascha Kegreiß
CTO HENSOLDT Cyber

Fotos: HENSOLDT Cyber

Pressekontakt & Bildanfragen
Simone Rudow
Tel.: +49 (0) 174 218 8102
simone.rudow@hensoldt-cyber.com