Drei Ebenen für IoT- und Embedded-Sicherheit

Kontron hat speziell für den Schutz von Endgeräten im industriellen Umfeld ein dreistufiges Secure-Systems-Konzept entwickelt. Teil dieses Konzepts ist die Security-Solution Approtect (eigene Schreibweise: APPROTECT). Approtect gliedert den komplexen Prozess der Absicherung von Endgeräten in kleine, je nach Bedarf individuell kombinierbare, Teilstücke.

Fachartikel von Norbert Hauser

ECKDATEN

Sicherheit ist der wichtigste Aspekt, um das Vertrauen der Anwender in den operativen Einsatz von Technologien zu gewinnen. In seinem Artikel geht Norbert Hauser von Kontron detailliert auf das Kontron Secure-Systems-Konzept ein.

Das Marktforschungsunternehmen Gartner rechnet damit, dass bis zum Jahr 2020 mehr als die Hälfte aller wichtigen Geschäftsprozesse auf die eine oder andere Weise mit dem Internet der Dinge (IoT) verknüpft sein wird. Dies führt laut Gartner auch dazu, dass die Anforderungen für die Implementierung dieser Applikationen in vielen Branchen und Einsatzfeldern steigen werden. Im Bereich Sicherheit rechnen die Forscher mit einem ganz erheblichen Mehraufwand. Sie prognostizieren, dass der Anteil des Budgets für den Schutz von Operational Technology (OT) und Information Technology (IT) von derzeit lediglich einem auf 20 Prozent des gesamten IT-Sicherheitsbudgets im Jahr 2020 steigen wird.

Für Unternehmen, Behörden und Organisationen gehört es zur Pflicht, nicht nur die Vorteile des Internet der Dinge, von Industrie 4.0, Smart Home und Co. anzupreisen, sondern mindestens das gleiche Augenmerk auf die damit verbundenen Risiken zu legen. Aufgabe von Komponentenanbietern ist es, Lösungen und Systeme zur Risikominimierung nicht nur anzubieten, sondern auch ihre einfache und kostengünstige Implementierung zu ermöglichen.

Das Kontron Secure-Systems-Konzept

Kontron hat deshalb Ende 2016 eine erste Lösung eingeführt, die speziell für den Schutz von Endgeräten im industriellen Einsatz entwickelt wurde. Die Security Solution Approtect ist seitdem in allen neuen Kontron-Produkten standardmäßig enthalten und lässt sich teilweise auch bei bereits implementierten Komponenten einfach nachrüsten. Sie ist eine Säule des Anfang 2017 vorgestellten dreistufigen Secure-Systems-Konzepts. Dieses Konzept sorgt für Sicherheit bei Endgeräten von der Datenaufnahme bis zur Übergabe der Daten an das Gateway; vom Start des Device über die Anwendungsausführung bis hin zur Datensicherung.

Das Kontron Secure-System-Konzept: dreistufige Sicherheit für Embedded- und IoT-Systeme vom Systemstart bis zu den Anwendungsdaten.
(Bild: Kontron)

Sicherheit ist der wichtigste Aspekt, um das Vertrauen der Anwender in den operativen Einsatz von Technologien zu gewinnen. Das gilt für heute schon verfügbare Applikationen, ist aber noch zentraler für den Einsatz von neuen Anwendungen im IoT, der Smart Factory oder Industrie 4.0 und in der Medizintechnik. Nur wenn Unternehmen Vertrauen in die neuen Möglichkeiten haben, werden sie diese auch nutzen und von ihren Vorteilen profitieren.

Um sichere Embedded-Systeme verwirklichen zu können, hat Kontron das Secure-Systems-Konzept entwickelt. Es beruht auf drei Stufen: der Absicherung des BIOS, des Betriebssystems sowie der Anwendungen und ihrer Daten. Damit werden drei essenziell wichtige System-Ebenen der Kunden geschützt, sodass sie sich nicht länger Sorgen um die Sicherheit ihrer Daten machen müssen.

Für den Schutz der BIOS-Ebene setzt Kontron auf etablierte Standards.

Für den Schutz der BIOS-Ebene setzt Kontron auf etablierte Standards. Sichere Firmware-Updates und die Absicherung des Boot-Prozesses über die TPM 2.0 Hardware (Trusted Platform Module) stellen sicher, dass während des Boot-Vorgangs nur vorher signierte und verifizierte Programme ausgeführt werden. Nicht autorisierter und damit potenziell schädlicher Code, der andernfalls zur Manipulation des Endgeräts genutzt werden könnte, wird ignoriert. Ungewollte Veränderungen an BIOS oder Boot-Loader sind so nicht mehr möglich. Secure/Trusted Boot dient aber nicht nur dem Schutz der BIOS-Ebene, es fungiert insbesondere als Wegbereiter und Garant für die Ausführung eines sicheren Betriebssystems.

Betriebssystemschutz beim Ein- und Ausschalten

Als sicheres Betriebssystem nutzt Kontron Windows 10 IoT. Diese speziell für die Verwendung im IoT-Umfeld entwickelte Version von Windows 10 bietet umfangreiche Schutzmechanismen für das System und die von ihm verarbeiteten Unternehmensdaten. Sicherheitsfunktionen wie Secure Boot, Bit Locker, Device Guard und Credential Guard sorgen in Verbindung mit dem TPM 2.0 Chip dafür, dass das System während der Start- und Ausschaltphase gegen Angriffe abgesichert ist.

Daten und Anwendungen schützen

Zur Absicherung der Anwendungsebene setzt Kontron auf die Security Solution „Approtect – powered by Wibu“. Bei dieser Lösung

Sicherheit von Anwendungsdaten sowie des Programmcodes sorgt. Mittlerweile verbaut Kontron den Chip, der vom Partner Wibu-Systems bereitgestellt wird, in jedem seiner neuen Module und Motherboards. Damit haben Anwender die Freiheit, selbst zu entscheiden, ob sie die Sicherheitsfunktionen aktivieren wollen. Ältere Systeme können per Nachrüstset ebenfalls mit dem Chip ausgestattet werden.

Das COMe-cSL6 unterstützt mit einem integrierten Security-Chip von Wibu die Embedded-Security-Solution von Kontron.
(Bild: Kontron)

Der Binärcode der Anwendung wird so verschlüsselt, dass Reverse Engineering, also der einfache „Nachbau“ des Programms, unmöglich wird (IP Protection). Darüber hinaus stellt die kontinuierliche Überprüfung der Verschlüsselung sicher, dass die Anwendung auch wirklich nur auf den dafür vorgesehenen Geräten ausgeführt werden kann (Copy Protection).

Für Kontron ist die IT-Sicherheit im IoT ein zentrales Element der Digitalisierungsstrategie seiner Kunden und deshalb als Standard in allen Produkten serienmäßig enthalten. Eine Hardware-Basis, die Sicherheitsmechanismen schon von Haus aus integriert, vereinfacht den Implementierungsprozess von IoT-Anwendungen enorm, macht die Produktentwicklung effizienter und die Kunden-Designs zukunftssicher. Bestehende Systeme können per Nachrüstkits auf Basis von „mPCIe“-Modulen oder USB-Sticks mit der Lösung ausgerüstet werden.

Auf der nächsten Seite: Approtect im Detail

Leitgedanke bei der Entwicklung von Approtect war es, den komplexen Prozess der Absicherung von Endgeräten in günstigere kleine, je nach Bedarf individuell kombinierbare, Teilstücke zu gliedern. So lassen sich auch spezifische Sicherheitsanforderungen abdecken, ohne zum Ressourcenfresser zu werden. Kunden sind nicht länger gezwungen, sich mit teuren Investitionen vor unendlich vielen, für sie teils hypothetischen Bedrohungsszenarien zu schützen.

Der in der Security Solution verwendete Sicherheitschip verfügt über einen Kontrollmechanismus, der die Verschlüsselung der Anwendung überprüft. So wird sichergestellt, dass das Programm auch wirklich nur von den dafür vorgesehenen Geräten ausgeführt werden kann. Durch einen stetigen Austausch mit dem Chip, der im laufenden Betrieb kontinuierlich Teile der Applikation entschlüsselt, wird zudem dafür gesorgt, dass Anwendungsdaten nicht einfach aus dem Arbeitsspeicher ausgelesen werden können. Damit sind die Anwendungen geschützt ohne zusätzlichen Kompilierungsaufwand oder komplizierte Schlüsselverwaltungsprozesse.

Mit Approtect Licensing lassen sich zusätzlich neue Geschäftsmodelle etablieren und durchsetzen. So ließen sich beispielweise einzelne Anwendungsfunktionen auf einen bestimmten Zeitraum oder eine definierte Ausführungszahl beschränken. Nützlich ist dies für Testszenarien, aber auch andere innovative Einsatzmöglichkeiten sind denkbar. Der Kreativität sind dabei keine Grenzen gesetzt.

Kontron und S&T für noch mehr Sicherheit

Durch den im August 2017 besiegelten Zusammenschluss mit der S&T-Gruppe baut Kontron seine Sicherheitskompetenzen weiter aus. Kunden erhalten in Zukunft ein erweitertes Portfolio umfassender Lösungen in den Bereichen Embedded-Module, Boards und Systeme, Internet der Dinge und Industrie 4.0. Insgesamt arbeiten damit im Unternehmensverbund rund 2300 erfahrene Ingenieure im OT- und IT-Bereich an Lösungen für die nahtlose und sichere Verbindung von Embedded-Systemen in die Embedded- oder Public-Cloud.

Die Sicherheit von Daten und Anwendungen, besonders im IoT-Umfeld, können durch die Verschmelzung von Kontron mit S&T zukünftig noch besser gewährleistet werden. Zum einen, weil jetzt noch mehr Ingenieure an der Weiterentwicklung von Sicherheitslösungen arbeiten; zum anderen, weil Kontron künftig noch mehr Komponenten aus einer Hand anbieten kann. Die Kunden erhalten so eine durchgängige und mit allen Schnittstellen kompatible Infrastruktur. Das erhöht das Sicherheitsniveau bei nur minimalem Implementierungsaufwand erheblich.
(ah)

ÜBER DEN AUTOR

Norbert Hauser
Vice President Marketing, Kontron

WEITERE INFOS

Kontron

86156 Augsburg

Deutschland

Zum Firmenprofil ›