

SICHER HEIT

IM FOKUS

Ganzheitliche Security
für Smart Connected Products

DIE SITUATION

DAS ENDE VON „NEVER TOUCH A RUNNING SYSTEM“

Der Erfolg von Internet of Things und Mobile Devices erfasst mehr und mehr Anwendungsbereiche. Datengetriebene Services und Geschäftsmodelle rund um Smart Connected Products haben mittlerweile einen entscheidenden Einfluss auf den Markterfolg eines Unternehmens. Das verändert auch die Sicht auf die Geräte grundlegend.

In der Vergangenheit waren Embedded Geräte isoliert und wurden nur mit dem Mindestmaß an Software betrieben. Durch die Integration von Connectivity in die Geräte kommen neue Anforderungen an die Pflege der Gerätesoftware hinzu. Die Geräte sind jetzt von überall erreichbar und somit angreifbar.

Der Einsatz weit verbreiteter Standardsoftware, wie beispielsweise Linux, bringt nicht nur Vorteile mit sich, sondern macht auch standardisierte Angriffe möglich. Die durch SW-Bibliotheken und weitere Dienste gestiegene Komplexität der Geräte bietet mehr Angriffsfläche. Eine Vielzahl von in den Medien dokumentierten Beispielen auch namhafter Gerätehersteller zeigen, dass diese Schwächen systematisch gefunden und ausgenutzt werden.

DIE HERAUSFORDERUNG

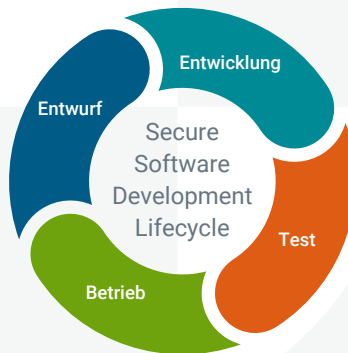
VERNETZTE GERÄTE SCHNELL UND SICHER ENTWICKELN

Zwar ist nicht jedes Gerät ein Hochsicherheitsprodukt, dennoch kann mangelnde Sicherheit zu immensen Schäden für den Hersteller führen. Außerdem gilt es wertvolle Daten zu schützen – aus eigenem Interesse oder von Rechts wegen (DSGVO).

Es ist essentiell Security ganzheitlich zu betrachten. Das bedeutet, dass Sie Security in Ihren Produktentwicklungsprozess integrieren müssen.

Nur so können Sie das Potential – welches in der Vernetzung und Erreichbarkeit der Geräte steckt – erschließen, um diese über ihre ganze Lebenszeit sicher zu betreiben.

Gleichzeitig soll aber weiterhin Funktionalität schnell und effizient an Kundenanforderungen angepasst werden, ohne dabei die Gerätesicherheit zu kompromittieren. Security darf nicht zum Stolperstein oder Bremsklotz für Ihre Entwicklung werden.



UNSERE LÖSUNG

SICHER VOM ANFANG BIS ZUM ENDE

Wir betrachten Sicherheit ganzheitlich über den Lebenszyklus der Geräte und den Entwicklungsprozess.

Wir bieten Ihnen off-the-shelf Lösungen rund um Security für den gesamten Device Lifecycle:

Security Canvas

Wir visualisieren die maßgeblichen Sicherheitsaspekte Ihres Gerätes oder Ihrer Lösung. Der Security Canvas wird zum Sicherheitswerkzeug Ihrer Teams.

Threat & Risk Analyse

Wir erkennen Bedrohungen, beurteilen Risiken und finden entsprechende Gegenmaßnahmen.

Sichere Entwicklung

Unsere Experten helfen Ihren Entwicklern, das Sicherheitsniveau Ihres Codes kontinuierlich zu verbessern. Bei Bedarf unterstützen wir Sie außerdem bei der Umsetzung von Sicherheitsmaßnahmen.

Automatisierung

Wir helfen dabei, die Sicherheit des Geräts durch automatisierte Analysen und Tests zu erhöhen. So können Ihre Entwickler effizient arbeiten.

Device Lifecycle Management / Over-the-Air Update

Wir begleiten Sie bei der Integration eines Secure Software Development Lifecycles in Ihre Geräteentwicklung mit fertigen Diensten für Gerätemanagement und Software-Updates.

KEINE ANGST VOR SECURITY



Rundum sorglos

Wir betreuen und begleiten Sie von A bis Z – von der Bestimmung des sinnvollen Sicherheitsniveaus bis zum Betrieb.



Vertrauen durch Erfahrung

Wir machen Ihre Smart Connected Products sicher. Dabei können Sie auf unsere langjährige Securityerfahrung vertrauen.



Zeit für Ihr Kerngeschäft

Wir halten Ihnen und Ihrem Team den Rücken frei. So wird Security nicht zum Stolperstein und Sie können sich auf Ihre Kernaufgaben konzentrieren.



Minimiertes Risiko

Mit unseren Lösungen für den Lebenszyklus Ihrer Geräte und zur Etablierung eines Secure Software Development Lifecycles reduzieren Sie Sicherheitsrisiken.



🏠 complement AG
Südwestpark 92
90449 Nürnberg

✉ info@complement.de

☎ +49 911 25 50 976 0

www.complement.de