NTSecuritySolutions

Creating safety.
With passion.

NewTec

NTSecurityAnalysis

Angreifer- und Bedrohungsanalyse: Cyber-Risiken für vernetzte Embedded-Geräte systematisch minimieren

www.newtec.de

Warum NTSecurityAnalysis?

Hersteller vernetzter Embedded-Geräte müssen heute zwingend Fragen der IT-Sicherheit in ihre Produktstrategie einbeziehen:

Schaden vermeiden: Die Zahl von Cyber-Angriffen auf IoT-Geräte wächst seit Jahren. Schon aus Haftungsgründen dürfen Hersteller dieses Thema nicht auf die leichte Schulter nehmen, denn unsichere IoT-Komponenten können erheblichen Schaden anrichten.

Auswirkungen auf Safety: Beeinträchtigungen der IT-Sicherheit (Security) gefährden auch die funktionale Sicherheit (Safety), wenn Hacker etwa Systeme sabotieren oder die Kontrolle übernehmen.

Normen erfüllen: Deshalb fordert auch die Safety-Grundnorm IEC 61508 explizit Security-Schwachstellenanalysen für bedrohte elektronische Systeme. Sie verweist dazu auf die branchenübergreifende Security-Normenreihe IEC 62443. Auch der EU Cybersecurity Act schreibt „Security by Design" und „Security by Default" als Regelungsprinzipien für sicherheitsrelevante Produkte fest.

Ihr Vorteil: Cyber-Risiken für vernetzte Embedded-Geräte systematisch minimieren

- Entscheidungsunterstützung durch konkreten Maßnahmenkatalog (Security Requirements Dokumente – SR)
- Einstieg in IEC 62443-konformen Security-Management-Prozess
- Kein Aufbau eigener Security-Kompetenzen erforderlich
- Strukturierter und schneller Prozess
- Kooperation aller Projekt-Stakeholder
- Schnellere Zertifizierung

Was ist NTSecurityAnalysis?

NewTec betrachtet Sicherheit als Einheit: Safety & Security by Design. Ziel von NTSecurityAnalysis ist es, relevante Security-Risiken für existierende oder neu entwickelte, vernetzte Embedded-Geräte systematisch zu ermitteln, zu bewerten und angemessen zu behandeln. Unser Analyseansatz berücksichtigt alle relevanten Perspektiven auf die Sicherheit Ihres Systems:

- Vorhandener Produktentstehungsprozess inkl. Safety-Entwicklung
- Projekt-Stakeholder aus unterschiedlichen Bereichen
- Zu schützende Systeme entlang des kompletten Product Lifecycle
- Konkreter Schutzbedarf Ihrer Assets
- Normen und Vorschriften
- Realistische Risikobewertung
- Ökonomische Risikobehandlung

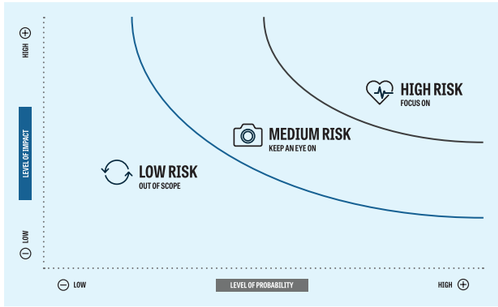
Die erfahrenen NewTec-Experten orientieren sich dabei an bewährten Best Practices, den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und den internationalen Grundnormen für die sichere Systementwicklung IEC 62443 (Security) und IEC 61508 (Safety). Wir haben unseren Security-Management-Prozess eng mit dem TÜV abgestimmt, um Zertifizierungen zu erleichtern und zu beschleunigen.

Wie funktioniert NTSecurityAnalysis?

In zwei separaten Sessions identifizieren wir gemeinsam mit Ihnen relevante Cyber-Gefährdungen (Schwachstellen und Bedrohungen), bewerten die damit einhergehenden Risiken und bestimmen Maßnahmen, wie Sie diese Gefährdungen auf ein akzeptables Restrisiko reduzieren.

Phase 1: Systemanalyse (2 Tage)

- **Systemarchitektur und Struktur**
  Analyse des Gerätes und seiner Umgebung inkl. Hard- und Softwarekomponenten, Schnittstellen/Protokollen und Daten
- **Schutzbedarfsanalyse (Assets)**
  Auswahl der wichtigsten Zielobjekte für Absicherungsmaßnahmen
- **Normenlage**
  Anforderungen der IEC 62443 für die konkreten Anwendungen



Phase 2: Bedrohungsanalyse und Risikobehandlung (3–5 Tage)

- **Schutzziele und Schutzbedarf**
  Feststellung des Schutzbedarfs aller Assets (Vertraulichkeit, Integrität, Verfügbarkeit) unter Berücksichtigung typischer Anwendungen und Schadensszenarien
- **Bedrohungsanalyse und Angreiferprofile**
  Beschreibung möglicher Bedrohungen (gerichtete Angriffe, ungerichtete Bedrohungen, Schutz vor IP-Diebstahl, ...) und typischer Angreifer
- **Risikoanalyse und Priorisierung**
  Bewertung von Eintrittswahrscheinlichkeit und Schadenspotenzial für jede Bedrohung
- **Risikobehandlung (Maßnahmenkatalog)**
  Kriterien zum Umgang mit den analysierten Risiken (Minimierung, Transfer, Akzeptanz); Reduktion von Eintrittswahrscheinlichkeit oder Schadenswirkung auf ein vertretbares Restrisiko durch geeignete Maßnahmen
- **Nächste Schritte**
  Empfehlungen für das weitere Vorgehen mit grober Aufwandsabschätzung
- **Auswertung und Dokumentation**
  Zusammenfassung der Ergebnisse als Entscheidungsgrundlage für die Planung, Security Requirements und Measures (SR).

Creating safety.
With passion.

NewTec

NewTec GmbH
Hauptsitz Ulm
Buchenweg 3
89284 Pfaffenhofen a. d. Roth
Germany
☎ +49 7302 9611-0
✉ info@newtec.de
🖵 www.newtec.de

Bremen · Friedrichshafen · Freiburg · Mannheim

F870_0323