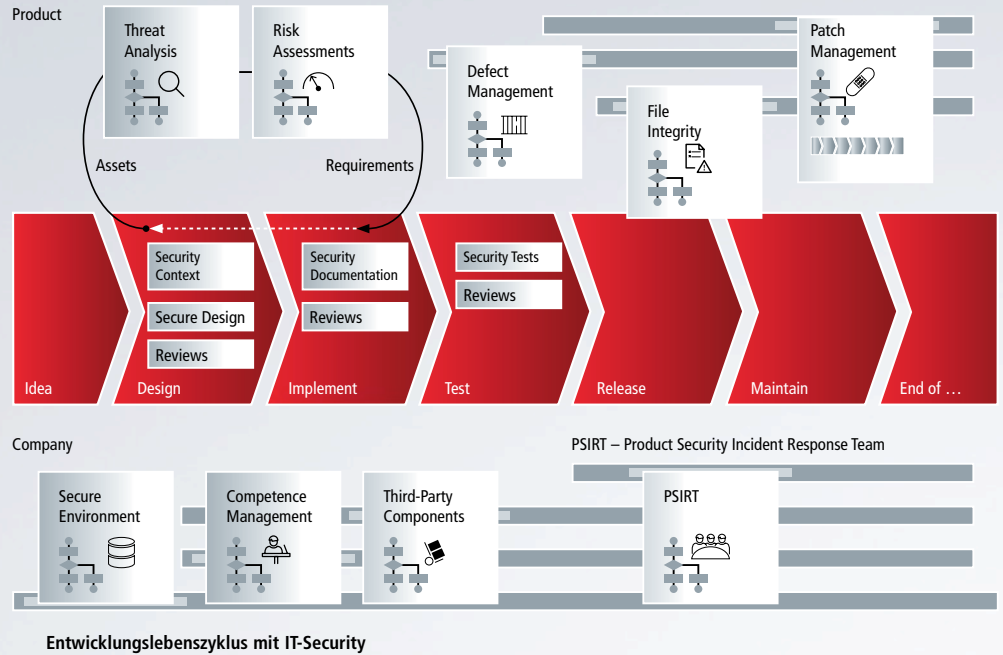


Aspekte der IT-Security frühzeitig im Blick

Die frühe Entscheidung, TwinCAT als PC-basierte Steuerung auf Betriebssystemen aus der IT-Branche zu realisieren, hat sich auch bezüglich der IT-Security als vorteilhaft erwiesen. Denn massentaugliche Funktionen für die IT-Security erschienen zuerst für solche Systeme und konnten deshalb oft direkt mit TwinCAT verwendet werden. Andere Steuerungstechnologien mit proprietärer Firmware haben hingegen Security-Eigenschaften erst ganzheitlich entwickelt, nachdem der Computerwurm Stuxnet entdeckt wurde.



Security-Funktionen können nur dann effektiv sein, wenn sie in einer Anlage rechtzeitig eingeplant und verwendet werden. Hierzu stellt Beckhoff für seine Produkte Hilfe bereit, z. B. mit dem kontinuierlich erweiterten Security-Leitfaden für IPCs, der inzwischen mehrere Betriebssystemgenerationen behandelt. Zudem wurde für die Produkte ein Lebenszyklus etabliert, in den von der Produktidee bis zur Abkündigung die IT-Security ganzheitlich eingewebt ist. Dieser Lebenszyklus wurde und wird kontinuierlich verbessert. Es sind Security-Eigenschaften in Produkten entstanden und weitere Prozesse zum Nutzen der Anwender. Entwicklungswerkzeuge von Beckhoff unterstützen Ingenieure bei ähnlichen Vorhaben, u. a. durch Source Control im TwinCAT-Engineering (TE1000).

Zu den Produkteigenschaften zählen beispielsweise das verschlüsselte Protokoll Secure ADS zur Kommunikation zwischen allen Instanzen von TwinCAT, die über Sicherheitsprotokolle wie TLS geschützte Kommunikation bei TwinCAT IoT Communication (TF6701), die Mechanismen zum Know-how-Schutz von Quelltexten und Projekten im Engineering und zur Laufzeit per Software Protection sowie die per HTTPS-Protokoll geschützte Kommunikation bei TwinCAT HMI (TE2000). In TwinCAT OPC UA (TF6100) sind zudem nahezu alle Security-Funktionen des zugehörigen Standards umgesetzt.

Einerseits tragen Eigenschaften von Produkten zur IT-Security bei, andererseits gelebte Prozesse in der gesamten Lieferkette. Als vertrauenswürdiger Lieferant zählt Beckhoff hierzu z. B. die regelmäßige Bereitstellung von Informationen über Betriebssystem-Updates, die auf Kompatibilität mit TwinCAT 3 getestet wurden, sowie den Prozess zur Behandlung und Veröffentlichung von Sicherheitslücken. Beckhoff hat frühzeitig ein eigenes Product Security Incident

Response Team (PSIRT) aufgebaut, mit sicheren Kommunikationskanälen zu Kunden, Security-Analysten und nationalen wie internationalen Stellen, welche die Behandlung von Sicherheitslücken koordinieren. Die IT-Sicherheitsplattform CERT@VDE vom VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V. wurde mit Unterstützung von Beckhoff ins Leben gerufen. Kleine und mittlere Unternehmen (KMU) aus dem Bereich der Automatisierungstechnik können darüber Unterstützung hinsichtlich IT-Sicherheitsthemen erhalten.

Aber nicht nur an Funktionen und Prozesse ist bei TwinCAT gedacht worden, sondern auch an Grundsätze: Bei der Weiterentwicklung werden bestehende und neue Voreinstellungen derart gestaltet, dass sie bereits „secure“ sind, dem Grundsatz „Secure by Default“ folgend.



Torsten Förder,
Produktmanagement TwinCAT,
Security

weitere Infos unter:

www.beckhoff.com/secguide

www.beckhoff.com/secinfo