Die Cyber Resiliance Act (CRA) Konformität von INSEVIS-Produkten

1. Einordnung des Cyber Resilience Acts (CRA)

Der Cyber Resilience Act (CRA) ist eine EU-Verordnung, die verbindliche Anforderungen an die Cybersicherheit von Produkten mit digitalen Komponenten definiert. Ziel der Verordnung ist es, sicherzustellen, dass diese Produkte über ihren gesamten Lebenszyklus hinweg sicher konzipiert, entwickelt, betrieben und gewartet werden . Als Hersteller industrieller Automatisierungstechnik unterstützt INSEVIS die Zielsetzungen des CRA ausdrücklich.
INSEVIS hat einen internen Schwachstellenbehandlungs- und Bekanntgabeprozess erstellt, der eine Meldeinfrastruktur für Schwachstellen beinhaltet. SBoms für alle Produkte erlauben eine Schwachstellenüberwachung bei entsprechenden Portalen. Jedes Produkt wurde einer Bedrohungsanalyse unterzogen und die Handlungsempfehlungen zur Erreichung einer CRA-Konformität in den folgenden Punkten dargelegt.

2. IT-Sicherheits- und Integrationsrichtlinie (CRA-Konformität)

- **Produktstatus:** Die INSEVIS-Produkte sind als Legacy-Produkte klassifiziert. Sie verfügen über digitale Elemente, unterstützen jedoch werkseitig keine nativen Verschlüsselungsprotokolle (z. B. Transportverschlüsselung via TLS/HTTPS).
- **Kompensationspflicht:** Um ein unkritisches Risiko-Niveau im Gesamtsystem zu erreichen, muss die fehlende produktspezifische Härtung durch eine **isolierte und geschützte Systemumgebung** ausgeglichen werden.

3. Zwingende Netzwerkkapselung (Kompensation der Unverschlüsselung)

Da die Datenübertragung der INSEVIS-Komponenten unverschlüsselt erfolgt, ist das Abhören und Manipulieren von Datenpaketen im Netzwerk rein physikalisch möglich. Der Kunde muss diese Eigenschaft durch folgende ausgleichende Maßnahmen kompensieren:

- **Physikalische oder logische Isolation:** Die Steuerung darf unter keinen Umständen direkt mit einem übergeordneten Unternehmensnetzwerk (Office-LAN) oder dem Internet verbunden werden. Sie ist in einem vollständig isolierten OT-Netzsegment (VLAN gemäß **IEC 62443**) zu betreiben.
- **Einsatz von Sicherheits-Gateways:** Sollte eine Kommunikation mit externen Systemen erforderlich sein, muss der Kunde der Steuerung ein dediziertes Sicherheits-Gateway (z. B. VPN-Appliance, Industrial Firewall mit Deep Packet Inspection) vorschalten. Die Verschlüsselung der Datenstrecke (z. B. via IPsec oder OpenVPN) muss zwingend auf diesem Gateway erfolgen.
- **Protokoll-Whitelisting:** Auf der vorgeschalteten Firewall sind ausschließlich die für den Betrieb zwingend erforderlichen, unverschlüsselten Ports (z. B. Modbus/TCP, native Feldbus-Protokolle) gerätespezifisch freizugeben. Jeder andere Netzwerkverkehr ist zu blockieren.

4. Verschärfter physischer und logischer Zugriffsschutz

Da die Komponente über keine modernen Identitäts- und Zugriffsmanagementsysteme (wie MFA oder rollenbasierte RBAC) verfügt, muss der Zugriff auf Systemebene kontrolliert werden:

- **Mechanischer Schutzbereich:** Die Steuerung muss in einem verschlossenen Schaltschrank der Schutzklasse **mindestens IP54** mit dokumentiertem Schlüsselsystem verbaut werden. Der physische Zugriff ist auf autorisiertes Fachpersonal zu beschränken.
- **Schnittstellen-Absicherung:** Lokale Service-Schnittstellen (z. B. serielle Ports, RJ45-Diagnoseports) dürfen nicht nach außen geführt werden. Sie müssen innerhalb des verschlossenen Schaltschranks verbleiben.

- **Vorschalt-Authentifizierung:** Vor-Ort-Bedienplätze (z. B. HMIs), die direkt mit der unverschlüsselten Steuerung kommunizieren, müssen zwingend über ein eigenes, CRA-konformes Benutzermanagement mit Passwort-Richtlinien verfügen, um unberechtigte Befehlseingaben an die Steuerung zu verhindern.

5. Patch-Management und Obsoleszenz-Strategie

- **Eingeschränktes Update-Verfahren:** Firmware-Aktualisierungen dienen bei Legacy-Produkten primär der Fehlerbehebung und funktionalen Stabilität. Neue Sicherheitsfeatures (wie nachträgliche Verschlüsselung) werden für diese Hardware-Generation nicht bereitgestellt.
- **Risikoüberwachung:** Der Kunde ist verpflichtet, die vom Hersteller bereitgestellten Sicherheitswarnungen (Advisories) zu überwachen und die vorgeschalteten Sicherheitskomponenten (Firewalls/Gateways) bei neu bekannt gewordenen Bedrohungslagen anzupassen.

6. Produktlebenszyklus und Support-Zeiträume (Lifecycle-Daten)

Gemäß den regulatorischen Vorgaben des Cyber Resilience Acts (CRA) werden für INSEVIS-Produkte verbindlichen Ankündigungen und Fristen. Der Kunde muss diese Daten in der Risikoanalyse und Betriebsplanung des Gesamtsystems berücksichtigen:

- **End of Sale (EoS) – Vertriebsende**
  (Ab diesem Datum ist die Komponente nicht mehr für den regulären Neuvertrieb verfügbar.)
- **End of Life (EoL) – Produktlebensende**
  (Die reguläre Produktpflege wird eingestellt. Ersatzteile sind ab diesem Zeitpunkt nur noch eingeschränkt verfügbar.)
- **End of Support (EoS) – Supportende für Sicherheitsupdates**
  (Bis zu diesem Datum stellt der Hersteller kritische Sicherheitswarnungen (Advisories) und Updates zur Fehlerbehebung bereit. Nach Ablauf dieses Datums erfolgt keine technische Unterstützung und keine Bereitstellung von Software-Patches mehr. Das Gesamtsystem muss nach diesem Termin durch zusätzliche, kundenseitige Maßnahmen abgesichert oder die Komponente ausgetauscht werden.)
- **Sichere Außerbetriebnahme** mit sicherer Entfernung der Nutzerdaten durch „Factory Reset“ bei Linux-basierten Geräten bzw. „Clear All + IP-Löschen“ bei OT-Geräten mit INSEVIS-Firmware.

7. Konformitätserklärung für das Gesamtsystem

Bitte beachten:

- Eine CRA-Konformität ersetzt keine System- oder Maschinenverantwortung. Die CRA Durchführungsverordnung ist an das Produkt adressiert und nicht an das vollständige Maschinensystem.
- Die sichere Konfiguration und der Betrieb liegen weiterhin in Mitverantwortung des Betreibers. Der Kunde (Systemintegrator) wird darauf hingewiesen, dass die Einhaltung dieser Richtlinie integraler Bestandteil der Risikoanalyse für seine Gesamtanlage ist. Bei Nichtbeachtung der Kapselungsvorgaben erlischt die Konformitätsvermutung des Gesamtsystems bezüglich der CRA-Anforderungen für unkritische Systemumgebungen.

Erlangen, den 12.Juni 2026

Jörg Peters
Baasansuren Sodnompil
Bastian Süß