Akuter Handlungsbedarf für den Maschinen- und Anlagenbau

Neue Cybersecurity-Anforderungen für den Export in die USA

In seiner Executive Order zur Verbesserung der Cybersicherheit der Nation vom 12. Mai 2021, hat US-Präsident Joe Biden unter anderem die Verbesserung der Softwarelieferkette gefordert.

Daraus lassen sich **neue Cybersecurity-Anforderungen** ableiten, die weltweit Hersteller und Exporteure von sicherheitsrelevanten Maschinen in die USA betreffen. ("… and those that run the vital machinery that ensures our safety (operational technology)").

Wie fit ist Ihre Softwareentwicklung? Wir haben Ihnen für ein schnelles Selbstassessment eine **Checkliste** aus den in der Executive Order geforderten Maßnahmen/Anforderungen beigefügt.

Eines wird mit dieser Executive Order und anderen kürzlich erschienenen Publikationen deutlich: das Thema Cybersecurity wird nun auch in der Produktentwicklung (noch) wichtiger.

Gerne stehe ich Ihnen für einen unverbindlichen Austausch zur Verfügung.

Jana Karina von Wedel
Head of Cybersecurity & Principal Consultant

Cybersecurity Website
cybersecurity@invensity.com

INVENSITY betreut im Bereich Cybersecurity erfolgreich zahlreiche Kunden bei der Produktentwicklung im Maschinen- und Anlagenbau.

Darüber hinaus entwickeln wir – speziell für den Anwendungsfall im Mittelstand – eigene Software-Applikationen zu Cybersecurity und Open-Source-Software Compliance. So zum Beispiel eine Applikation für die Erstellung von Threat Analyses and Risk Assessments (TARAs), wie sie z.B. von den IT-Sicherheitsnormen IEC 62443 und ISO 27001 gefordert wird.

Zudem entwickeln wir aktuell eine Software-Applikation für eine effiziente Automatisierung des OSS Compliance Managements. Unsere Applikationen ermöglichen unsere eigenen Trainings-, Beratungs- und Engineeringtätigkeiten besser & effizienter[1] zu gestalten. Dank des Einsatzes unserer Software Applikation können Kunden dabei im Anschluss an unsere Beratungsunterstützung die erarbeitete Vorgehensweise systematisch bei neuen Projekten erfolgreich anwenden.

Mit weltweit über 200 Mitarbeitern und Projekten bei mittlerweile über 150 namhaften Kunden, vereinen wir seit über 14 Jahren erfolgreich Engineering- und technische Beratungsexpertise.

innovation made by talents

[1] Gemäß einem Kunden beträgt die Zeitersparnis bei der Erstellung einer TARA durch die Übersichtlichkeit und die Wiederverwendbarkeit ca. 50% für den Cybersecurityengineer. Noch wichtiger für den Kunden waren dabei andere Aspekte: Cybersecurity Prozesssicherheit sowie Risikotransparenz für Kunden & Assessoren.

Checkliste

Anforderungen aus der Executive Order

“The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The Secretary of Commerce acting through the Director of NIST** shall issue guidance. Such guidance shall include standards, procedures, or criteria regarding: […]

	Anforderung / Maßnahme	Ja	Nein	Kommentar
i.	secure software development environments, including such actions as:			
	employing encryption for data; and			
	monitoring operations and alerts and responding to attempted and actual cyber incidents;			
ii.	generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes […]			
iii	employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;			
iv	employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release			
v	providing, when requested by a purchaser, artifacts of the execution of the tools and processes […], and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;			
vi	maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;			
vii	providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;			
F.viii	participating in a vulnerability disclosure program that includes a reporting and disclosure process;			
F.ix	attesting to conformity with secure software development practices; and			
F.x	ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.			

innovation made by talents