AMDT
PRODUCTION RESILIENCE DELIVERED

Whitepaper

Ein Überblick über die EU Cybersicherheitsanforderungen

NIS-2: Verschärfte Cybersicherheit in der Produktion

Empfindliche Strafen ab 2024:
Wissen Sie, ob Ihr Unternehmen compliant ist?

VORWORT

Unsere Handlungsempfehlungen und Lösungsansätze zur neuen EU-Direktive im Überblick

Zehn Millionen Euro oder zwei Prozent des weltweit im Vorjahr getätigten Umsatzes – mit diesem maximalen Strafmaß will die EU wesentliche Einrichtungen zur Einhaltung neuer Cybersicherheitsstandards bringen. Die neue Cybersicherheitsdirektive soll Angriffe abwenden und Schäden minimieren, um Wirtschaft und Gesellschaft vor Ausfällen und deren Folgen zu schützen.

Diese neuen Vorgaben haben nicht nur Auswirkungen auf die Betreiber kritischer Infrastrukturen an sich, sondern erstrecken sich jetzt auch auf die Industrie und erhöhen indirekt die Sicherheitsanforderungen an alle Unternehmen, die Ziel von Angriffen werden könnten.

Auf einen Blick: wie die EU Industrie und Versorger mit NIS-2 zum Handeln drängt

- Verschärftes, verpflichtendes, vorsorgliches Sicherheitsmanagement und Meldepflichten bei Sicherheitsvorfällen
- NIS-2 betrifft alle Unternehmen der darin definierten „kritischen“ und „wichtigen“ Sektoren, die Dienste und Produkte für Einwohner und Unternehmen in der EU anbieten – auch wenn die Anbieter selbst ihren **Sitz außerhalb der EU** haben, beispielsweise in den USA
- Risiken: Bußgelder bei Verstößen, je nach Sektor und Schwere des Verstoßes zwischen sieben und zehn Millionen Euro oder bis zu zwei Prozent des weltweiten Jahresumsatzes.

Diese Handlungsempfehlungen richten sich an Betreiber kritischer Infrastrukturen, die ihre Sicherheitsanforderungen durch die neuen EU-Direktive erhöhen wollen, um Wirtschaft und Gesellschaft vor Ausfällen und deren Folgen zu schützen.

Hintergrund: Digitalisierung und Sicherheit in der OT

Mit der Digitalisierung und Automatisierung von Infrastruktur und Produktion steigern Unternehmen und Organisationen ihre Effizienz und schaffen neue Potenziale. Die Transformation von Informationstechnologie und operational Technologie (OT) hat sich in den zurückliegenden Jahren noch deutlich beschleunigt, nicht zuletzt durch die Pandemie.

Parallel zum Digitalisierungsgrad haben Angriffe auf Produktion und Infrastruktur in den vergangenen Jahren deutlich zugenommen. Beispiele sind die gezielte Manipulation einer Trinkwasseraufbereitung in den USA und Angriffe auf Teile des Energienetzes in Europa.

Zugleich haben Ereignisse in den vergangenen Jahren aufgezeigt, wie tiefgreifend die Auswirkungen von unterbrochenen Lieferketten und beeinträchtigter Grundversorgung sind. Die Energie- und Gesundheitsversorgung, aber auch die Produktion wichtiger Grundstoffe und Vorprodukte ist eine wesentliche Säule unserer Gesellschaft und jeder Mangel, jede Unterbrechung oder Störung kann gesamtgesellschaftliche Schäden zur Folge haben.

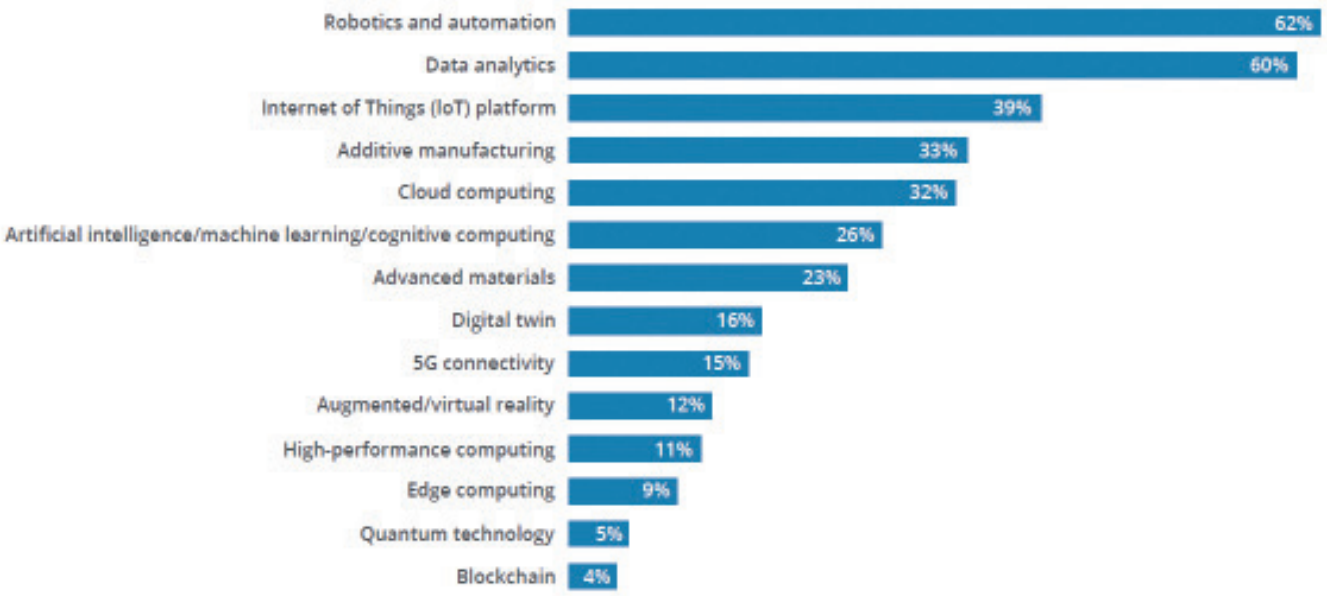


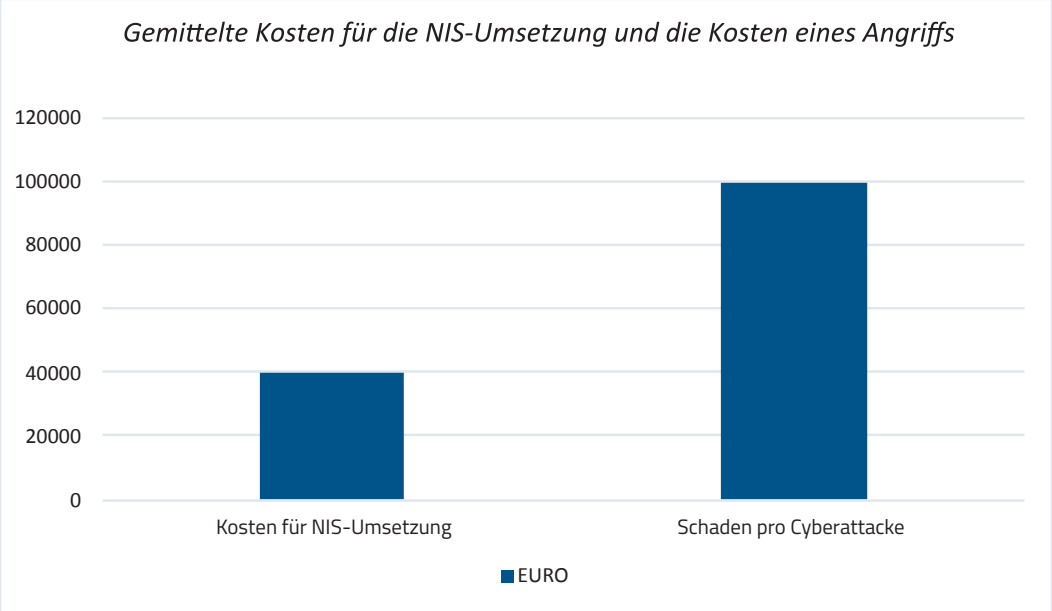
Abb. 1: Laut dem 2023 Manufacturing Industry Outlook | Deloitte US haben sich Unternehmen mit einem höheren Digitalisierungsgrad als widerstandsfähiger erwiesen. Ihre Investitionen in die Digitalisierung konzentrieren sich laut Befragung in den nächsten 12 Monaten auf eine Reihe von Technologien, um die betriebliche Effizienz zu steigern. Quelle: 2023 Deloitte manufacturing outlook survey

NIS und NIS-2 – die Zeitleiste

Im Mittel gaben befragte Unternehmen 40.000 Euro für die Umsetzung der Vorgaben aus, während die „European Union Agency for Cybersecurity“ (ENISA) die Kosten eines Angriffs auf durchschnittlich 100.000 Euro schätzt. Das Sicherheitsunternehmen Sophos beziffert die Kosten eines Angriffs speziell auf produzierende Unternehmen im Report „The State of Ransomware in Manufacturing and Production 2021“ gar auf 1,5 Millionen Dollar.

2016	2018	2020	2022	2023	2024
Beschluss NIS	NIS in Kraft	Vorschlag NIS-2	Beschluss NIS-2	NIS-2 in Kraft	Umsetzung in nationales Recht

DREI JAHRE NACH INKRAFT-TRETEN VON NIS HATTEN NUR VIER VON FÜNF UNTERNEHMEN DIE VORGABEN UMGESETZT.



Quellen: ENISA und Sophos