Wie steht es um die Cyber-Resilienz?

Prof. Dr. Dennis-Kenji Kipker spricht im Interview über Herausforderungen für die Datensicherheit. Ist eine adäquate Regulierung dieser schnelllebigen Materie überhaupt möglich und welche Rolle spielt NIS2?

© privat

Prof. Dr. Dennis-Kenji Kipker ist wissenschaftlicher Direktor des cyberintelligence.institute in Frankfurt a.M. sowie Gastprofessor an der privaten, durch die Soros Foundation begründeten Riga Graduate School of Law in Lettland. Kipker ist Berater der Bundesregierung und der Europäischen Kommission sowie Mitglied im Advisory Board von NordVPN.

Compliance: Was ist aus Ihrer Sicht die aktuell drängendste Herausforderung bzw. die größte Gefahr in der IT-Sicherheit?
Kipker: Definitiv die digitale Lieferkette. Wo wir einerseits immer stärker auf Cloud Computing – auch mit dem Aufstieg der künstlichen Intelligenz – zurückgreifen, sind wir uns kaum der damit verbundenen Vulnerabilitäten bewusst, wenn betriebskritische Dienste in der digitalen Lieferkette ausfallen. Hinzu tritt, dass gerade die Hersteller und Betreiber dem Thema oftmals zu wenig Beachtung schenken.

Compliance: Wie bewerten Sie die Versuche – insbesondere auf europäischer Ebene –, den rasanten technischen Wandel adäquat mit zielgenauer Regulierung zu begleiten? Ist das überhaupt möglich?
Kipker: Eine Regulierung ist notwendig, um der schnellen technischen Entwicklung einen verbindlichen Rahmen zu geben. Zwangsläufig kann Regulierung nicht sämtliche Herausforderungen und Risiken von Technologie vollständig antizipieren, aber zumindest dazu beitragen, bestehende Risiken zu erkennen und einzudämmen. Hinreichend technologieoffene Rechtsvorschriften können somit entscheidend dazu beitragen, Technologie vertrauenswürdiger zu machen.

Compliance: Gilt das auch für NIS2? Worin besteht der Nutzen von NIS2 für deutsche Unternehmen?
Kipker: NIS2 allein wird nicht zu mehr flächendeckender unternehmerischer Cybersicherheit führen – dennoch ist die Regulierung unerlässlich, um für tausende Unternehmen einen ersten Ansatzpunkt zu liefern, sich tiefergehend mit der Cybersicherheit zu befassen. Richtig in eine Unternehmensstruktur implementiert kann NIS2 entscheidend dazu beitragen, die Vulnerabilitäten in ebenjener digitalen Lieferkette zu reduzieren.

Compliance: Haben Sie dennoch Kritikpunkte in Bezug auf NIS2 bzw. die Umsetzung in Deutschland?
Kipker: Man könnte jetzt natürlich den ausufernden nationalen Zeitplan kritisieren, davon möchte ich aber absehen, da es dabei nicht um inhaltliche Fragen geht. Ich würde mir gerade im Hinblick auf die konkreten Cybersecurity Measurements mehr Technologie- und damit Anpassungsoffenheit wünschen. Aber hier war eigentlich schon die EU selbst inkonsequent, indem sie in NIS2 einen mehr oder weniger willkürlichen Katalog an Umsetzungsmaßnahmen zusammengestellt hat, der mehr Unsicherheit als Klarstellung bringt. Und genau das führt am Ende zu Umsetzungsdefiziten in der Cybersicherheit.

Das Interview führte Christina Kahlen-Pappas.

Einen ausführlichen Vortrag von Prof. Dr. Dennis-Kenji Kipker zu Cyber-Resilienz, NIS2, Kritis-DG & Co können Sie bei der Deutschen Compliance-Konferenz am 13. und 14. Mai 2025 in Frankfurt am Main erleben.