EXPERTENINTERVIEW

NIS2 und das neue Verantwortungsmodell in der Zugriffs-Governance

Guido Kraft
Field CISO, WALLIX

Mehr als 20 Jahre Erfahrung in den Bereichen Cybersicherheit, Corporate Governance, ISO 27001, TISAX und operative Sicherheitsprogramme für kritische Infrastrukturen und regulierte Umgebungen.

Q Wie verändert NIS2 die Beziehung zwischen CISO, Geschäftsleitung und Vorstand?

Mit NIS2 ist Cybersicherheit nicht länger nur ein IT-Thema, sondern wird zu einem echten Geschäftsrisiko. Die Geschäftsleitung und der Vorstand tragen nun direkte Verantwortung für die Cybersicherheitsmaßnahmen und die Resilienz der Organisation.Dadurch verändert sich auch die Rolle des CISO: Er wird zur Schnittstelle zwischen technischen Teams und strategischer Unternehmensführung. Gleichzeitig muss der Vorstand eine aktivere Aufsicht übernehmen, Cyberrisiken verstehen und die richtigen Fragen stellen.

Q Warum gewinnt die Zugriffs-Governance mit NIS2 zunehmend an Bedeutung?

Nahezu alles in IT- und OT-Umgebungen basiert auf Zugriffen. Risiken entstehen immer dann, wenn Benutzer mehr Rechte besitzen als erforderlich oder Berechtigungen nicht mit den tatsächlichen Verantwortlichkeiten übereinstimmen. Die Zugriffs-Governance definiert, wer auf welche Ressourcen zugreifen darf, unter welchen Bedingungen und mit welchem Verantwortungsniveau. Deshalb sollten Unternehmen sie als strategische Sicherheitsebene betrachten, die sowohl die Sicherheit als auch die Compliance stärkt.

EXPERTENINTERVIEW

wallix

Welche Hindernisse erschweren öffentlichen Organisationen die Einführung einer stärkeren Zugriffs-Governance?

Die größten Herausforderungen sind Legacy-Systeme, fragmentierte IT-Landschaften und begrenzte Budgets. Viele ältere Anwendungen unterstützen keine modernen Zugriffsmodelle, wodurch gemeinsam genutzte Konten und übermäßige Berechtigungen bestehen bleiben. Dennoch lassen sich Sicherheitskontrollen durch Privileged Access Management, starke Authentifizierung und nachvollziehbare Zugriffe deutlich verbessern.

Wie sollten Unternehmen unter NIS2 Prävention und Incident Investigation ausbalancieren?

Prävention und Untersuchung sind gleichermaßen wichtig. Unternehmen brauchen Sicherheitsmaßnahmen, die Risiken reduzieren und gleichzeitig Transparenz sowie Nachvollziehbarkeit im Ernstfall gewährleisten. Security-Teams müssen jederzeit nachvollziehen können, wer worauf zugegriffen hat und welche Aktionen durchgeführt wurden.

Warum sind gemeinsam genutzte Administratorkonten noch immer so verbreitet?

Gemeinsam genutzte Konten entstehen oft durch Legacy-Systeme und operative Anforderungen. Wo möglich, sollten Unternehmen auf individuelle Benutzerkonten umstellen. Andernfalls müssen privilegierte Zugriffe kontrolliert werden, um Transparenz und Sicherheit zu gewährleisten.

Wie sollte ein effektives Drittanbieterzugriffs-Management unter NIS2 aussehen?

Der Zugriff externer Dienstleister sollte genauso streng verwaltet werden wie interne privilegierte Zugriffe. Wichtig sind zeitlich begrenzte Berechtigungen, kontinuierliche Überwachung und vollständige Nachvollziehbarkeit. Unternehmen sollten unüberwachte externe Zugriffe und dauerhafte Berechtigungen vermeiden.

Sollten Unternehmen NIS2 primär aus Compliance- oder Resilienzsicht angehen?

Der beste Ansatz besteht darin, NIS2 als Chance zur Stärkung der operativen Resilienz zu betrachten – nicht nur als Compliance-Anforderung.

Wenn Unternehmen ihre Transparenz, ihre Zugriffs-Governance und ihre operative Disziplin verbessern, wird Compliance zu einer natürlichen Folge besserer Sicherheitskontrollen.

Worauf könnte sich die nächste große europäische Cybersicherheitsregulierung konzentrieren?

Voraussichtlich wird der nächste große Schwerpunkt auf der Governance von KI liegen.

Je stärker künstliche Intelligenz in Geschäftsprozesse integriert wird, desto wichtiger werden klare Richtlinien für Datennutzung, Verantwortlichkeiten, Risikomanagement und regulatorische Compliance.