Experte: Mittelstand sollte neue NIS2-Vorschriften für Cyberresilienz ab Oktober ernst nehmen

Cybersicherheit: Dringender Handlungsbedarf für 30.000 Firmen

Die deutsche Wirtschaft muss sich dringend auf die neuen Anforderungen zur Cyberresilienz aus dem NIS2-Umsetzungs- und Cybersicherheitsstärkungs-gesetz (NIS2UmsuCG) vorbereiten, mahnt Dennis Weyel, International Technical Director mit Zuständigkeit für Europa beim Sicherheitsunternehmen Horizon3.ai. NIS2 – das Kürzel steht für „Netzwerk- und Informationssicherheit“ – wird rund 30.000 Unternehmen in Deutschland betreffen, schätzt der Cybersicherheitsexperte. „Die Zeit drängt“, sagt Dennis Weyel, weil mit dem Inkrafttreten zum Oktober dieses Jahres zu rechnen sei.

40 Prozent aller Firmen ab 50 Beschäftigte sind betroffen

Nach Einschätzung des Sicherheitsfachmanns gehen weite Teile vor allem der mittelständischen Wirtschaft davon aus, von NIS2 nicht betroffen zu sein, weil die neue Richtlinie nur für die Betreiber sogenannter Kritischer Infrastrukturen (KRITIS) gelte. „Das ist ein Irrtum. In Wirklichkeit unterliegen rund 40 Prozent aller Firmen ab 50 Beschäftigte in Deutschland den NIS2-Regularien“, sagt Dennis Weyel. Unter die Richtlinie fallen nämlich nicht nur die Unternehmen in den vom Gesetzgeber genannten Branchen, sondern auch alle Zulieferer und Dienstleister dazu.

Die betroffenen Branchen sind Abfall- und Abwasserwirtschaft, Bankwesen, Chemie, digitale Infrastruktur, Energiewirtschaft, Finanzwesen, Forschung, Gesundheitswesen, IKT-Dienstleistungen, Lebensmittel, Medizinprodukte, Öffentliche Verwaltung, Post- und Kurierdienste, Transport, Trinkwasser, Weltraum, Maschinen, Fahrzeuge und elektrische/elektronische Geräte. „Firmen, die Unternehmen aus einer dieser Branchen im Kundenkreis haben, sollten sich auf jeden Fall auf NIS2 vorbereiten“, empfiehlt Dennis Weyel.

Die Erfüllung der vom Gesetzgeber verlangten NIS2-Anforderungen wird vielen mittelständischen Unternehmen schwerfallen, befürchtet der Sicherheitsexperte. Er zählt auf, womit sich Firmen alles beschäftigen müssen, um den NIS2-Kriterien zu genügen: Risikobewertungen, Sicherheitsvorfälle, Kryptografie, IT-Sicherheitstrainings, Sicherheit bei der IT-Beschaffung, Authentifizierung, Beschäftigte mit Zugang zu sensiblen Informationen, Betriebsführung während und nach einem Sicherheitsvorfall, Supply Chain ¬und Wirksamkeit aller dieser Sicherheitsmaßnahmen.

Experte empfiehlt regelmäßige Penetrationstests

Daher empfiehlt der Sicherheitsexperte dem Mittelstand, die eigene Infrastruktur mit hoher Regelmäßigkeit sogenannten Penetrationstests zu unterziehen. Bei den im Fachjargon „Pentests“ genannten Maßnahmen wird im Firmenauftrag ein Generalangriff aus dem Internet auf die eigene IT-Infrastruktur durchgeführt.

„Es gibt wohl keinen besseren Weg als eine umfassende Attacke auf das eigene Netzwerk, um dessen Widerstandsfähigkeit in der Praxis zu überprüfen“, erklärt Dennis Weyel, dessen Sicherheitsfirma Horizon3.ai selbst eine Cloudplattform für Pentesting betreibt. Er erläutert: „Auf dem Bankensektor sind Pentests in Form von Stresstests durch die EZB schon jahrelang Usus. Rechtzeitig vor dem NIS2-Start können nun auch kleine und mittlere Firmen via Cloud diese Königsdisziplin der Cybersicherheitsüberprüfung für sich in Anspruch nehmen.“
Nach Einschätzung des Sicherheitsfachmanns decken regelmäßige Penetrationstests wesentliche NIS2-Anforderungen ab. „Ein professioneller Angriff auf die eigene IT-Infrastruktur stellt wohl die ehrlichste Form der Risikobewertung dar“, sagt er.

Nicht genug Pentesting-Experten, um die Nachfrage zu decken

Diejenigen, die Penetrationstests durchführen, sind hochqualifizierte Experten mit Zertifizierungen wie OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker) und vielen anderen. Die Herausforderung für Unternehmen besteht darin, dass es nicht genügend zertifizierte Penetrationstester gibt, um den Bedarf zu decken. Aus diesem Grund suchen Unternehmen nach Lösungen, die es ihnen ermöglichen, selbst Pentests durchzuführen, indem sie autonome Pentesting-Plattformen wie NodeZero verwenden, um die NIS2-Anforderungen zu erfüllen.