Umfrage: NIS2 kennt nur jeder zweite Befragte

Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) hat der TÜV-Verband im Juni eine neue repräsentative Umfrage zur Cybersicherheit in Unternehmen vorgestellt. Die Ergebnisse seien in zweifacher Hinsicht besorgniserregend, fasst das BSI in einer Mitteilung zusammen: „Zum einen konnte ein Anstieg der Bedrohungslage verzeichnet werden, zum anderen zeigen die Umfrageergebnisse, dass viele Firmen die Lage unterschätzen und die eigene Resilienz überbewerten." Das BSI warnt vor trügerischer Sicherheit.

NIS2? Nie gehört! Nur jeder zweite kennt die EU-Richtlinie.

Nur etwa die Hälfte der Befragten habe angegeben, die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS2) zu kennen. Mit der Umsetzung der NIS2-Richtlinie in nationales Recht, die aufgrund der vorgezogenen Neuwahlen in Deutschland bisher nicht erfolgt ist, werde das BSI für deutlich mehr Unternehmen als zuvor Aufsichtsbehörde. Für die bestehenden Kritischen Infrastrukturen (KRITIS) ändere sich hierdurch voraussichtlich wenig, aber für ca. 29.000 nach der NIS2-Richtlinie „wesentliche" (essential entities) und „wichtige" Einrichtungen (important entities) ergäben sich erstmals gesetzliche Pflichten, gibt das BSI zu Bedenken.

Der TÜV-Verband ergänzt: „Neun von zehn (91 Prozent) Unternehmen bewerten ihre Cybersicherheit als gut oder sehr gut. Und jedes vierte Unternehmen (27 Prozent) gibt an, dass IT-Sicherheit für sie nur eine kleine oder gar keine Rolle spielt." Eine Mehrheit spreche sich für gesetzliche Vorgaben aus, um das Schutzniveau in der Wirtschaft zu erhöhen: 56 Prozent seien der Meinung, dass alle Unternehmen verpflichtet sein sollten, angemessene Maßnahmen für ihre Cybersecurity zu ergreifen. Die Bundesregierung solle die überfällige nationale Umsetzung der NIS2-Richtlinie zügig verabschieden.

Einen Entwurf hierfür hat die neue Regierungskoalition inzwischen auf den Weg gebracht (siehe hierzu unseren Aufmacher in dieser Ausgabe auf Seite 2 „NIS2-Umsetzung à la Deutschland: Ein Lehrstück in verpassten Chancen".

Die Studie des TÜV-Verbandes zeige, dass auf dem Weg zur Cybernation Deutschland noch eine Menge Arbeit vor uns liegt, so das Resümee beim BSI. Für Besorgnis sorgt dort vor allem die geringe Bekanntheit der NIS2-Richtlinie. Umso wichtiger sei ihre zügige Umsetzung in nationales Recht. Die damit einhergehende Bürokratie und der Mehraufwand für Unternehmen, könne trotz aller Kritik an zusätzlichem Aufwand dabei helfen, die Resilienz der deutschen Wirtschaft umfassend zu erhöhen. Das BSI lege seinen Schwerpunkt dabei auf Hilfestellung und Kooperation und unterstütze Unternehmen auch heute schon mit umfangreichen Informations- und Beratungsangeboten. Das Credo laute „Cybersicherheit vor Bürokratie".

Auch der TÜV-Verband will in Sachen Cybersicherheit unterstützen und spricht unter anderem folgende Empfehlungen für Unternehmen aus:

1. Cyberrisiken ernst nehmen
   Unternehmen sollten eine qualifizierte Risikoanalyse durchführen und diese angesichts des dynamischen technologischen und geopolitischen Umfelds regelmäßig aktualisieren. Was ist besonders zu schützen? Welche Bedrohungen gibt es? Was sind potenzielle Schwachstellen im Unternehmen? Diese und weitere Fragen gelte es zu beantworten. Je nach Größe, Branche und Tätigkeitsgebiet könnten Cyberrisiken sehr unterschiedlich bewertet werden.
2. Cybersecurity-Strategie entwickeln
   Übergeordnetes Ziel der Strategie sei es, ein angemessenes Sicherheitslevel für das jeweilige Unternehmen zu definieren. Bestandteil dessen sollte eine IT-Sicherheitsrichtlinie sein. In dieser werden messbare Ziele definiert, konkrete Sicherheitsanforderungen festgelegt und klare Verantwortlichkeiten geschaffen. Sie sei die Basis für die Maßnahmenplanung.
3. Maßnahmenplan ausarbeiten
   Auf Grundlage der Risikoanalyse und strategischer Überlegungen sollten konkrete Maßnahmen festgelegt werden.

Nicht zu unterschätzen seien Lieferketten als Einfallstor: 10 Prozent der Unternehmen wurden über Zulieferer oder Kunden attackiert. Zwar stellen 32 Prozent der Unternehmen Sicherheitsanforderungen an Partner – eine echte Auditierung sei allerdings selten, stellt der TÜV-Verband fest.

chk

IMPRESSUM
Verlag
Deutscher Fachverlag GmbH, Mainzer Landstraße 251,
60326 Frankfurt am Main
Registergericht AG Frankfurt am Main HRB 8501
USt-IdNr. DE 114139662
Geschäftsführung: Peter Esser (Sprecher), Thomas Berner, Markus Gotta
Aufsichtsrat: Andreas Lorch, Catrin Lorch, Dr. Edith Baumann-Lorch, Peter Ruß
Redaktion: Christina Kahlen-Pappas (verantwortlich),
Telefon: 0151 27 24 56 63, E-Mail: christina.kahlen-pappas@dfv.de
Verlagsleitung: RA Torsten Kutschke,
Telefon: 069 7595-1151, E-Mail: torsten.kutschke@dfv.de
Anzeigen: Mikhail Tsyganov,
Telefon: 069 7595-2779, E-Mail: Mikhail.Tsyganov@dfv.de
Fachbeirat: Gregor Barendregt, Carl Zeiss AG; Andrea Berneis, Berneis Legal & Compliance; Ralf Brandt, dievini patch Beteiligungs GmbH; Joern-Ulrich Fink, Regulatory Adherence & Compliance Policy Governance, Deutsche Bank AG; Otto Geiß, Deutsches Netzwerk Wirtschaftsethik; Mirko Haase, Hilti Corporation; Prof. Dr. Katharina Hastenrath, ZHAW Zürcher Hochschule für Angewandte Wissenschaften; Corina Käsler, Senior Advisor, State Street Bank International GmbH; Dr. Karsten Leffrang, General Counsel Germany, Valeo; Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt/Oder; Thomas Muth, Muth-zur-Entwicklung; Stephan Niermann; Dr. Dietmar Prechtel, Osram GmbH; Dr. Alexander von Reden, Global Compliance, Miele Group; Hartmut T. Renz, Partner STRATECO GmbH; Dr. Barbara Roth, State Street Bank International; Jörg Siegmund, Getzner Textil AG; Eric S. Soong, Group Head Compliance & Corporate Security, Schaeffler Technologies AG & Co. KG; Dr. Martin Walter, selbstständiger Autor, Berater und Referent für Compliance-Themen
Jahresabonnement: kostenlos
Erscheinungsweise: monatlich (10 Ausgaben pro Jahr)
Layout: Uta Struhalla-Kautz, SK-Grafik, www.sk-grafik.de