



Cyberrichtlinie NIS-2 verfehlt Wirkung

Neun von zehn betroffenen Unternehmen in NRW nicht vollständig vorbereitet

Bochum 18.03.2026. Trotz wachsender Cyberbedrohungen und hoher Eigenverantwortung bleibt die Umsetzung der EU-Sicherheitsrichtlinie NIS-2, die seit Dezember 2025 in Kraft getreten ist, weit hinter den Anforderungen zurück. Nur jedes zehnte Unternehmen in Nordrhein-Westfalen, das unter die NIS-2-Richtlinie fällt, hat die gesetzlichen Vorgaben vollständig umgesetzt. Rund 30 Prozent haben bislang keinerlei Maßnahmen ergriffen. Das geht aus einer aktuellen Auswertung von DIGITAL.SICHER.NRW auf Basis einer repräsentativen Studie von G DATA CyberDefense hervor.

Große Umsetzungslücke trotz gesetzlicher Vorgaben

Die Ergebnisse offenbaren einen deutlichen Widerspruch: Während sich Angestellte heute kompetenter denn je fühlen und die Mehrheit eine persönliche Verantwortung für IT-Sicherheit im eigenen Unternehmen sieht, bleibt die strukturelle und regulatorische Absicherung vielfach unzureichend.

KI verschärft die Bedrohungslage

Gleichzeitig nimmt die Bedrohungslage weiter zu. Zwei Drittel der Unternehmen in NRW erwarten, dass z.B. Gefahren im digitalen Raum wie Cyberangriffe durch den Einsatz Künstlicher Intelligenz künftig zunehmen. Dennoch schätzt rund die Hälfte der Betriebe das eigene Risiko, von Cyberkriminalität betroffen zu sein, als gering oder sehr gering ein – ein Wert, der in den vergangenen Jahren sogar gestiegen ist.

„Viele Beschäftigte fühlen sich heute sicherer und kompetenter im Umgang mit IT-Sicherheit. Das ist grundsätzlich positiv. Gleichzeitig zeigen die Ergebnisse, dass dieses Sicherheitsgefühl nicht automatisch in ausreichende Schutzmaßnahmen mündet. Gerade für kleine und mittlere Unternehmen gilt: Digitale Selbstverteidigung muss weder kompliziert noch teuer sein – wichtig ist, überhaupt anzufangen“, so Sebastian Barchnicki, Sprecher der Geschäftsführung bei DIGITAL.SICHER.NRW.

Schnelle Reaktion, aber hohe Schäden bei Cyberangriffen

Positiv fällt auf: Kommt es zu einem Sicherheitsvorfall, reagieren Unternehmen in NRW schnell. Im Bundesvergleich gelingt ihnen die Eindämmung von Cyberangriffen am zügigsten – meist innerhalb einer Woche. Die Folgen bleiben dennoch gravierend: Fast drei Viertel der Befragten berichten von spürbaren Auswirkungen wie Betriebsausfällen, Datenverlusten oder finanziellen Schäden.

Kleine und mittlere Unternehmen besonders gefordert

Besonders kleine und mittlere Unternehmen sehen Nachholbedarf. Sie bewerten den Reifegrad ihrer IT-Sicherheit niedriger als Großunternehmen

22. April 2026

Seite 1

Kompetenzzentrum
für Cybersicherheit
in der Wirtschaft
in Nordrhein-Westfalen

CYBERSEC-NRW gGmbH
Lise-Meitner-Allee 4
44801 Bochum
Telefon 0234 | 5200 7334

Standort Bonn:
Rheinwerkallee 6
53227 Bonn

Ihre Ansprechpartnerin:
Laura Schoner
presse@digital-sicher.nrw
+49 170 783 196 3

www.digital-sicher.nrw





und schätzen ihre Sicherheitskultur schwächer ein. Zudem stuft knapp die Hälfte aller Unternehmen den Fachkräftemangel im Bereich IT-Sicherheit als hoch oder sehr hoch ein.

„Mit der zunehmenden Digitalisierung wächst auch die Verantwortung der Unternehmen, ihre IT zuverlässig zu schützen,“ sagt Andreas Lüning, Vorstand und Mitgründer der G DATA CyberDefense AG. „IT-Sicherheit ist heute aber nicht nur mehr rein technisches Thema. Sie wird dann wirksam, wenn Technologie, klare Verantwortlichkeiten und ein starkes Sicherheitsbewusstsein im gesamten Unternehmen zusammenkommen.“

... Weitere Studienergebnisse sowie Angaben zur Methodik sind [hier](#) verfügbar.

Über das Kompetenzzentrum

... DIGITAL.SICHER.NRW ist das Kompetenzzentrum für Cybersicherheit in der Wirtschaft in NRW. Beauftragt vom Ministerium für Wirtschaft, Industrie, Klimaschutz und Energie des Landes NRW bietet es kostenfreie Beratungen, Webinare und Informationen zu den wichtigsten Präventionsmaßnahmen vor Cyberangriffen an. Mehr Informationen finden Sie unter: www.digital-sicher.nrw

