plusserver

NIS2 in a Nutshell

Wer ist betroffen und was ist zu tun?

Was ist NIS2?

Network and Information Security Directive 2 (NIS2)

Überführung in nationales Recht bis 17.10.2024	Angemessene Sicherheitsmaßnahmen für Organisationen in kritischen Sektoren	Bessere Zusammenarbeit der EU-Mitgliedsstaaten zur Stärkung der Cybersecurity in Europa	Sanktionen und hohe Geldstrafen bei Verstößen

Wen betrifft NIS2?

Dienstleistungen in der EU
50 MA. oder mind. 10 Mio. € Umsatz bzw. größenunabhängige Sonderfälle

Wesentliche Einrichtungen	Wichtige Einrichtungen
Energie	Post- und Kurierdienste
Verkehr und Transport	Abfallwirtschaft
Bankwesen und Finanzmärkte	Produktion, Herstellung und Handel mit chemischen Stoffen
Gesundheitswesen	Produktion, Verarbeitung und Handel von Lebensmitteln
Trinkwasser	Verarbeitendes Gewerbe, Herstellung von Waren
Abwasser	Anbieter digitaler Dienste
Digitale Infrastruktur	Forschung
ICT Service Management	
Öffentliche Verwaltung	
Weltraum	

Sanktionen bei Verstößen	
Mindestens zehn Millionen Euro oder 2 Prozent des weltweiten Umsatzes im Vorjahr	Mindestens sieben Millionen Euro oder 1,4 Prozent des weltweiten Umsatzes im Vorjahr

Was ist zu tun? (einige Beispiele)

Risikobewertung	Führen Sie regelmäßige Risikobewertungen durch, um die spezifischen Bedrohungen und Schwachstellen Ihres Unternehmens zu identifizieren.
Sicherheits-maßnahmen	Implementieren Sie angemessene Sicherheitsmaßnahmen auf Stand der Technik, einschließlich Zugriffskontrollen, Verschlüsselung und Monitoring.
Incident-Management	Schaffen Sie die Grundlage für eine wirkungsvolle Prävention, Detektion und Bewältigung von Cybervorfällen durch eine 24/7-Überwachung der Infrastruktur.
Incident Response Plan	Erstellen Sie einen gut durchdachten Zwischenfallreaktionsplan, um sicherzustellen, dass Sie auf Vorfälle effektiv reagieren können.
Schulung und Sensibilisierung	Schulen Sie Ihre Mitarbeitenden und stärken Sie die Awareness für Sicherheitsrisiken. Vermitteln Sie Best Practices, um menschliche Fehler zu minimieren.
Compliance-Management	Halten Sie sich über die aktuellen Entwicklungen in der Gesetzgebung bezüglich Cybersicherheit auf dem Laufenden und stellen Sie sicher, dass Ihre Organisation stets konform ist.
Supply-Chain-Management	Ebenso relevant wie Ihre eigenen Sicherheitsmaßnahmen sind die Maßnahmen Ihrer Zulieferer. Achten Sie besonders auf Zertifizierungen wie ISO 27001 sowie bei Cloud-Anbietern auf ein BSI-C5-Testat.
Business-Continuity-Management	Setzen Sie eine Distaster-Recovery-Strategie mit Wiederstellung z. B. mittels Cloud-Ressourcen um.
Externe Hilfe	Wenden Sie sich auch an externe Berater und Lösungsanbieter, um sicherzustellen, dass Sie alle Anforderungen der NIS2-Richtlinie erfüllen.

Wie kann plusserver unterstützen?

Security-Beratung/ Consulting

+ Feinkonzeption und Design von Security-Maßnahmen und Architekturen
+ Pentests und Audits

Security-Lösungen

+ SOC as a Service
+ EDR as a Service
+ Schwachstellenmanagement
+ Next Gen Firewall
+ DDoS-Schutz
+ Backup/Disaster Recovery

Zertifizierte Infrastruktur

+ Standorte in DE
+ ISO 27001
+ BSI C5 (Typ-II)

Kostenfreie Checkliste erhalten und Compliance-Sorgen abhaken

› Jetzt downloaden

plusserver
Eine souveräne, zukunftsfähige und sichere Cloud

Wir bieten deutschen Unternehmen eine datensouveräne und anbieterunabhängige Basis für ihre digitalen Geschäftsprozesse. Auf unseren sicheren, skalierbaren Cloud-Plattformen realisieren Kunden zukunftsfähige und kosteneffiziente digitale Anwendungen. Wir beraten unsere Kunden zu Cloud-Architekturen sowie zur Integration bestehender IT-Umgebungen. Dabei agieren wir schnell, dynamisch und stets persönlich.

Sie haben Fragen? Kontaktieren Sie uns.
Wir helfen gerne weiter.
Schnell und unkompliziert.

+49 2203 1045 3500
beratung@plusserver.com

BSI C5 CLOUD SECURITY · DATENSCHUTZ IDW PH 9.860.1 · ISAE 3402 · gaia-x · Sovereign Cloud Stack · TÜV SÜD · TÜV SÜD · JAN-2024