HORNETSECURITY BY proofpoint.

INFOSHEET AI POWERED

SO HILFT HORNETSECURITY BEI DER ERFÜLLUNG DER NIS2UMSUCG-ANFORDERUNGEN

Was ist die NIS2-Richtlinie?
Die NIS2-Richtlinie ist eine EU-weite Gesetzgebung, die das Niveau der Netzwerk- und Informationssicherheit in der Europäischen Union deutlich erhöht. Sie ersetzt die frühere NIS1-Richtlinie und erweitert deren Anwendungsbereich auf mehr Branchen, strengere Sicherheitsanforderungen und härtere Sanktionen. Ziel ist die Erhöhung der Cybersicherheits-Resilienz aller relevanten Organisationen in der EU.

- **Meldepflichten**
  Unternehmen müssen schwerwiegende Sicherheits- und Cybervorfälle unmittelbar melden.
- **Risikomanagement**
  Systematische Identifikation, Bewertung und Reduktion von IT- und Cyberrisiken ist Pflicht.
- **Management & Governance**
  Die unternehmerische Leitung ist verantwortlich für Sicherheitsstrategien, Überwachung und kontinuierliche Verbesserung.
- **Durchsetzung & Sanktionen**
  Behörden können Prüfungen durchführen und bei Nichteinhaltung Bußgelder, Anordnungen oder weitere Sanktionen verhängen.

info@hornetsecurity.com | www.hornetsecurity.com

01/26

HORNETSECURITY
BY proofpoint.

INFOSHEET
AI POWERED

NIS2-READY MIT UNTERSTÜTZUNG VON HORNETSECURITY

365 4 TOTAL PROTECTION

365 Total Protection Plan 4 ist die **zentrale, integrierte Security-Plattform von Hornetsecurity**, die dabei unterstützt die technischen, organisatorischen und dokumentarischen Anforderungen der **NIS2-Richtlinie** zu adressieren – von Prävention über Detektion bis hin zu Nachweisbarkeit und Compliance.

NIS2-BEREICH	HERAUSFORDERUNG / ANFORDERUNG	HORNETSECURITY-LÖSUNG 365 TOTAL PROTECTION	WIE SIE HILFT
MELDEPFLICHTEN	Sofortige Erkennung und Meldung von Sicherheitsvorfällen sowie Nachweisbarkeit	EMAIL ARCHIVING	Revisionssichere Aufbewahrung von E-Mails zur Beweissicherung und Unterstützung von Incident-Meldungen
		ADVANCED THREAT PROTECTION	Frühzeitige Erkennung von Phishing-, Malware- und gezielten E-Mail-Angriffsvektoren
RISIKOMANAGEMENT	Systematische Identifikation, Bewertung und Reduktion von Cyberrisiken	365 TOTAL BACKUP	Backup und Wiederherstellung zur Sicherstellung der Geschäftskontinuität
		DMARC REPORTING & MANAGEMENT	Reduzierung von Domain-Missbrauch, Phishing und CEO-Fraud durch Domain-Authentifizierung
		CONTINUITY SERVICE	Sicherstellung des E-Mail-Betriebs bei Ausfällen oder Sicherheitsvorfällen
		EMAIL ENCRYPTION	Schutz sensibler Kommunikation durch Sicherstellung von Vertraulichkeit und Integrität
MANAGEMENT & GOVERNANCE	Etablierung von Verantwortung, Reporting und Schulungsmaßnahmen	SECURITY AWARENESS	Individuelle Sensibilisierung der Mitarbeitenden inkl. Reports für CISOs und Management
		PERMISSION MANAGEMENT	Kontrollierte Verwaltung und Überwachung von Zugriffs- und Berechtigungsstrukturen
DURCHSETZUNG & SANKTIONEN	Nachweisbarkeit, Audit-Bereitschaft und Dokumentation	EMAIL ARCHIVING	Sicherer und revisionssicherer Aufbewahrungsnachweis für Audits und Prüfungen
		SECURITY AWARENESS	Dokumentierte Awareness- und Schulungsaktivitäten als Governance- und Compliance-Nachweis