CYBERSECURITY ETHICAL HACKING PENETRATION TESTING SCHULUNG

ISGroup
Information Security

NIS2 Compliance

Gap-Analyse, Remediation Plan und Schulung für dauerhafte Konformität

ZIEL

Pflichten und Fristen in ein Resilienzprogramm überführen

Die NIS2-Richtlinie verlangt nachweisbare Governance, Risikomanagement, technische Maßnahmen und Reaktionsfähigkeit.

ISGroup übersetzt Anforderungen in operative Prioritäten passend zu Organisation, Branche und Exposition.

ISGroup
Information Security

METHODE

Von der Gap-Analyse zu einem umsetzbaren, prüfbaren Plan

Bewertung

Wir erfassen Scope, Pflichten, Governance und bestehende Maßnahmen.

Remediation Plan

Wir ordnen Maßnahmen nach Risiko, Abhängigkeiten, Kosten und Fristen.

Umsetzung

Wir unterstützen Kontrollen, Verfahren, Schulung und Nachweissammlung.

ISGroup
Information Security

UMSETZUNG

Governance, Lieferkette, Vorfälle und Business Continuity

Der Weg umfasst Risiken, Lieferanten, Schwachstellen, Zugriffe, Backups und Incident Response.

Rollen und Verantwortlichkeiten des Managements werden mit Eskalations- und Berichtswegen formalisiert.

Schulungen und Übungen machen Maßnahmen im Alltag wirksam.

ISGroup
Information Security

STÄRKEN

GRC- und technische Kompetenz im selben Team

Abdeckung

Organisatorische, dokumentarische und technische Anforderungen gemeinsam bewertet.

Prioritäten

Maßnahmen nach realem Risiko und Umsetzungskapazität geordnet.

Nachweise

Entscheidungen, Kontrollen und Prüfungen für Audits dokumentiert.

ISGroup
Information Security

OUTPUT

Eine NIS2-Roadmap mit Verantwortlichen, Fristen und Nachweisen

Gap-Analyse zu den anwendbaren Anforderungen.

Priorisierter Remediation Plan mit Verantwortlichen und Fristen.

Nachweisregister für Maßnahmen, Schulung und Prüfungen.

Management Reporting zu Fortschritt und Restrisiko.

ISGroup
Information Security

Let's HACK together

ISGroup
Information Security

CF e P.IVA 04164220230
www.isgroup.it

TERMIN VEREINBAREN

sales@isgroup.it

+39 045 4853232