Im Ernstfall zählt jede Entscheidung.
Der Incident Response Plan von Argos.

Ein Incident Response Plan legt vorab fest, wer im Cyber-Ernstfall welche Schritte geht – mit klaren Abläufen, Rollen sowie Eskalations- und Kommunikationswegen. Argos erstellt ihn praxisnah, branchenspezifisch und abgestimmt auf Ihre Meldepflichten.

>600	100+	24/7	seit 1999	ISO 27001	NIS-2
Kunden	Security-Experten	Cyber Defense Center	Managed Security	TÜV-SÜD-zertifiziert	DSGVO- & ISO-27001-Nachweise unterstützt

Das leistet der Service für Sie.

Rollen & Eskalation

Eine klare Rollen- und Verantwortlichkeitsmatrix mit definierten Eskalations- und Kommunikationswegen – jeder weiß im Ernstfall, was zu tun ist.

Szenarien & Use-Cases

Konkrete Reaktionsstrategien für typische Angriffe wie Ransomware, Datenabfluss oder CEO-Fraud – statt abstrakter Prozessbeschreibungen ohne Praxisbezug.

Meldepflichten

Meldepflichten nach DSGVO, NIS-2 und KRITIS sind im Plan verankert – inklusive Kontaktlisten, damit Fristen im Ernstfall zuverlässig eingehalten werden.

Tabletop-Validierung

Der Plan wird per Tabletop-Übung unter realistischen Bedingungen validiert und laufend gepflegt – damit er im Ernstfall wirklich funktioniert.

Für wen: Für Unternehmen, die im Ernstfall strukturiert reagieren wollen – KRITIS- und NIS-2-Betreiber mit gesetzlichen Melde- und Reaktionspflichten sowie cyber-versicherte Unternehmen, deren Versicherer einen aktuellen Plan verlangt.

Wenn ein Angriff läuft, bleibt keine Zeit, Zuständigkeiten zu klären oder Meldefristen zu recherchieren.
Der IR-Plan von Argos gibt Ihrer Organisation im entscheidenden Moment Struktur: Sie handeln schnell und koordiniert statt hektisch – und halten gesetzliche Meldepflichten zuverlässig ein.

Auf Seite 2: der direkte Vergleich mit dem klassischen Ansatz →

Ihr direkter Draht: +49 89 45 24 24-100 · kontakt@argos.security

Argos Incident Response Plan vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos Incident Response Plan
Ernstfall	Zuständigkeiten werden erst im Angriff geklärt	**Rollen und Wege vorab definiert** Rollen- und Verantwortlichkeitsmatrix
Szenarien	Abstrakter Plan ohne konkrete Fälle	**Use-Cases für reale Angriffe** Ransomware, Datenabfluss, CEO-Fraud
Meldepflichten	Fristen werden im Stress recherchiert	**DSGVO, NIS-2 und KRITIS verankert** Inklusive Kontaktlisten
Praxistauglich	Plan besteht nur auf dem Papier	**Per Tabletop-Übung validiert** Unter realistischen Bedingungen geprüft
Aktualität	Plan veraltet nach der Erstellung	**Laufende Pflege inklusive** Auch als Nachweis für Cyber-Versicherer

Ihr Leistungsumfang im Überblick

- Erstellung oder Review Ihres Incident Response Plans
- Rollen- und Verantwortlichkeitsmatrix
- Definierte Eskalations- und Kommunikationswege
- Use-Cases für Ransomware, Datenabfluss und CEO-Fraud
- Verankerte Meldepflichten nach DSGVO, NIS-2 und KRITIS
- Validierung per Tabletop-Übung und laufende Pflege

Für Ihre Geschäftsleitung: Auswahlsorgfalt belegbar (ISO/IEC 27001 TÜV SÜD, seit 1999, >600 Kunden) · Überwachung erfüllbar (Reporting an die Geschäftsleitung) · Leistungsumfang vertraglich klar definiert.

Ihr Part: benannte Ansprechpartner und Dokumentenzugang – Rollen, Zuständigkeiten und Berichtswege werden gemeinsam festgelegt. Details (Leistungsbeschreibung, AVV/TOM) im Erstgespräch.

Souverän. Deutsch. Nachweisbar.

- Deutscher Anbieter – seit 1999, Sitz in München
- 100+ Security-Expertinnen und -Experten
- ISO/IEC 27001 zertifiziert (TÜV SÜD)
- Unterstützt NIS-2-, DORA- und ISO-27001-Nachweise
- DSGVO-konforme Verarbeitung – AVV (Art. 28) & TOM auf Anfrage
- Angebunden an das 24/7 Cyber Defense Center

So starten Sie mit dem Service

01
Analyse & Struktur

Wir erfassen Ihre Infrastruktur, Meldepflichten und internen Strukturen und legen die Grundstruktur des Plans branchenspezifisch fest.

02
Szenarien & Dokumentation

Rollen, Eskalations- und Kommunikationswege sowie Reaktionsstrategien für Szenarien wie Ransomware oder CEO-Fraud werden dokumentiert.

03
Übung & Pflege

Der Plan wird per Tabletop-Übung unter realistischen Bedingungen validiert und anschließend laufend aktuell gehalten – als belastbare Grundlage.

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie Incident Response Plan auf Ihre Organisation und Ihre Anforderungen zugeschnitten wird.

Dr. Nils Kaufmann
Chief Sales Officer

+49 89 45 24 24-100
kontakt@argos.security · www.argos.security

Mehr zur Leistung: argos.security/leistungen/incident-response-plan →

Termin buchen