Sauber zurück in den Normalbetrieb. Recovery und Wiederherstellung nach dem Vorfall.

Recovery und Wiederherstellung bringt Systeme und Daten nach einem Sicherheitsvorfall geordnet zurück in den Betrieb. Argos Security bereinigt kompromittierte Umgebungen, baut sie gehärtet neu auf und verifiziert die Kompromittierungsfreiheit vor dem Go-Live.

>600	<15 Min	≤30 Min	seit 1999	ISO 27001	100 %
Kunden	Erkennung (MTTD)	Rückmeldung (SLA)	Managed Security	TÜV-SÜD-zertifiziert	souveränes CDC ab Q1/2027

Das leistet der Service für Sie.

Bereinigung

Kompromittierte Systeme und Konten werden konsequent bereinigt – die Erkenntnisse aus der Forensik fließen direkt in Bereinigung und Härtung ein.

Gehärteter Neuaufbau

Betroffene Umgebungen werden aus vertrauenswürdigen Quellen gehärtet neu aufgebaut – eine saubere Basis, die den nächsten Angriff erschwert.

Priorisierter Wiederanlauf

Systeme werden nach Geschäftskritikalität priorisiert wiederhergestellt: geschäftskritische Anwendungen zuerst, ergänzt um Datenwiederherstellung aus sauberen Backups.

Verifizierter Go-Live

Vor der kontrollierten Wiederinbetriebnahme wird die Kompromittierungsfreiheit geprüft und bestätigt – inklusive Nachbetreuung und abgeleiteter Härtungsmaßnahmen.

Für wen: Für Unternehmen nach einem Sicherheitsvorfall, die einen sauberen, sicheren Wiederanlauf statt eines übereilten Schnellstarts anstreben.

Nach einem Vorfall ist der Druck groß – doch ein ungeprüfter Neustart holt den Angreifer über Hintertüren zurück. Argos bringt Ordnung in den Wiederanlauf: bereinigt, gehärtet aus vertrauenswürdigen Quellen neu aufgebaut und vor dem Go-Live verifiziert frei von Kompromittierung.

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

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

Bildmotiv: KI-generiertes Symbolbild

Argos Recovery und Wiederherstellung vs. klassischer Ansatz

der Vergleich auf einen Blick

Kriterium	Klassischer Ansatz	Argos Recovery und Wiederherstellung
Wiederanlauf	Übereilter Schnellstart unter Zeitdruck	**Geordnete Rückkehr in den Betrieb** Priorisiert nach Geschäftskritikalität
Hintertüren	Angreifer kehrt über Reste zurück	**Kompromittierungsfreiheit verifiziert** Geprüft und bestätigt vor dem Go-Live
Wiederaufbau	Alte Images, alte Schwächen	**Gehärtet aus vertrauenswürdigen Quellen**
Forensik	Wiederherstellung losgelöst von der Analyse	**Eng mit der Forensik verzahnt** Erkenntnisse fließen in Bereinigung und Härtung
Daten	Restore ohne Prüfung der Backups	**Rückholung aus sauberen Backups**

Ihr Leistungsumfang im Überblick

- Bereinigung kompromittierter Systeme und Konten
- Gehärteter Neuaufbau aus vertrauenswürdigen Quellen
- Wiederherstellung priorisiert nach Geschäftskritikalität
- Geprüfte Kompromittierungsfreiheit vor dem Go-Live
- Datenwiederherstellung aus sauberen Backups
- Abgeleitete Härtungsmaßnahmen und Nachbetreuung

Für Ihre Geschäftsleitung: Auswahlsorgfalt belegbar (ISO/IEC 27001 TÜV SÜD, seit 1999, >600 Kunden) · Überwachung erfüllbar (Reporting & Reviews) · SLAs vertraglich statt Best Effort.

Ihr Part: Ansprechpartner & Zugänge im Onboarding – Rollen, Freigaben und Eingriffstiefe werden gemeinsam festgelegt. Details (RACI, SLA-Matrix, AVV/TOM) im Erstgespräch.

Souverän. Deutsch. Nachweisbar.

- SOC-Betrieb aus München – nach deutschem Recht
- Datenhaltung auf Wunsch vollständig in Deutschland
- ISO/IEC 27001 zertifiziert (TÜV SÜD)
- Unterstützt NIS-2-, DORA- und ISO-27001-Nachweise
- DSGVO-konforme Verarbeitung – AVV (Art. 28), TOM & Unterauftragsverarbeiter-Übersicht auf Anfrage
- Ab Q1/2027: 100 % souveränes Cyber Defense Center

So starten Sie mit dem Service

01
Lagebild & Priorisierung

Auf Basis der Forensik-Erkenntnisse werden betroffene Systeme erfasst und die Wiederherstellung nach Geschäftskritikalität priorisiert.

02
Bereinigung & Neuaufbau

Systeme und Konten werden bereinigt, gehärtet aus vertrauenswürdigen Quellen neu aufgebaut, Daten aus sauberen Backups zurückgeholt.

03
Verifizierter Go-Live

Vor der Wiederinbetriebnahme wird die Kompromittierungsfreiheit bestätigt; Argos begleitet den kontrollierten Go-Live samt Nachbetreuung.

> *„Als es passiert ist, hatten wir keine Zeit mehr nachzudenken. Ein Anruf und Argos hat übernommen. Ohne sie wäre das für uns ein ganz anderes Ende gewesen.“*
>
> Sebastian Altmann, CIO, Riva Engineering

Sprechen Sie mit uns, bevor es der Angreifer tut.

Vereinbaren Sie ein kostenloses 30-Minuten-Erstgespräch – Sie erfahren, wie Recovery und Wiederherstellung auf Ihre Infrastruktur und Bedrohungslage 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/recovery-wiederherstellung →

Termin buchen

Bildmotiv: KI-generiertes Symbolbild