Alles sicher wiederher-gestellt.

Die IT Disaster Recovery Architecture von CANCOM ist die beschleunigte und automatisierte Wiederherstellungsstrategie für den Ernstfall. Ob Cyberattacke, Erpressung mit Ransomware oder Ausfälle durch höhere Gewalt: IT Disaster Recovery Architecture von CANCOM ist viel mehr als ein herkömmliches Backup.

Die Lösung zeichnet sich durch umfangreiche Vorbereitung, unveränderbare Datenspeicher und eine zuverlässige Infrastruktur aus und ist „Made in Austria“ mit der branchen-bekannten Expertise der IT-Security- Profis von CANCOM. Wenn Sie sich fragen, ob Sie für den Fall der Fälle wirklich optimal gerüstet sind, finden Sie die Antwort hier zum Nachlesen – und noch besser in einem persönlichen Beratungsgespräch.

Ihr Mehrwert: Minimierung der Serviceunterbrechungen und des dadurch verursachten Schadens.

CANCOM

Business Continuity Consulting, zielgerichtete Infrastrukturanpassungen, rascher Zugriff auf Security-Expert:innen: die drei Bausteine der CANCOM IT Disaster Recovery Architecture.

Grundsätzlich definiert ein IT Disaster Recovery Management die technischen Strategien, Fähigkeiten, Pläne und Prozesse, um die festgelegten Business-Wiederherstellungspläne zu erreichen. Allerdings sind klassische IT-Disaster-Recovery-Architekturen wie Stretch-Datacenter oder Cluster beziehungsweise Daten-Spiegelung gegen Cyberattacken nicht wirksam, da diese nur auf bestimmte Technologiebereiche fokussiert sind und nicht das Ganze im Blick haben.

Die CANCOM IT Disaster Recovery Architecture erfasst hingegen sämtliche relevanten Bereiche und realisiert eine umfassende Lösung auf der Basis von drei synergetischen Denk- und Umsetzungsfeldern.

Consulting

Das österreichische Consulting mit integralem IT-Notfallplan.

Unsere Leistung umfasst die gesamte IT-Disaster-Planung vom Start mit einer Business Impact Analyse über das Aufsetzen von Governance-Prozessen rund um IT Disaster Recovery bis zur Planung und Durchführung von Wiederherstellungstests. Mit unserer Business-Impact-Analyse werden die Auswirkungen und die Kritikalität von Events auf den Geschäftsbetrieb identifiziert. Das Ergebnis bildet die Handlungsgrundlage zur Definition der Wiederherstellungsziele. In der sogenannten Continuity-Phase werden die notwendigen Prozesse und Begrifflichkeiten ausgearbeitet, um angemessen auf IT-Notfälle reagieren zu können. Zudem werden Richtlinien und Verantwortlichkeiten definiert. Diese Inhalte werden – neben weiteren generellen Lösungsansätzen – im Notfallhandbuch für die IT-Disaster-Wiederherstellung dokumentiert. Zum Projektabschluss werden durch unsere Governance-Leistungen weitere Optimierungspotenziale aufgezeigt sowie Gap-Analysen, Trainings und anderes mehr durchgeführt.

Infrastucture

Design und Automatisierung von IT Disaster Recovery in der Cloud oder On-Premises.

Im Zusammenspiel eines Recovery Orchestrators mit passender Hardware-Infrastruktur (On-Premises-Variante) oder Microsoft Azure (Cloud-Variante) und mit dem IT-Security-Know-how von CANCOM gelingt die sichere Wiederherstellung unternehmenskritischer Anwendungen und Systeme schnell und durchgängig. Nach dem Konzept einer „entkoppelten Systemlandschaft“ setzen wir auf einer vorhandenen Backup- und Recovery-Implementierung auf. Ein intaktes (immutable) Backup steht dann entweder auf gehärteten Systemen vor Ort oder in der Cloud zur Verfügung. Auf diese Weise wird sichergestellt, dass Daten innerhalb eines definierten Zeitraums nicht mehr veränderbar sind – und dies alles über ein kostengünstiges und doch hochperformatives Medium. Für den Fall der Fälle bereitet CANCOM gemeinsam mit Ihren Expert:innen einen Anlaufplan in einem Disaster Recovery Orchestrator auf. Die Wiederherstellung der Anwendungen geht dann auf Knopfdruck. Das bedeutet auch: Kosten für den Betrieb der Systeme fallen definitiv erst im Zuge des Recovery-Prozesses an.

Security

Incident Response direkt aus dem CANCOM Cyber Defense Center.

Protect, Prevent, Detect, Respond: Das Cyber Defense Center (CDC) von CANCOM ist ein weltweit genutztes Security Operation Center aus Österreich. Mit sechs verschiedenen IT-Security-Modulen sorgt das CDC dafür, dass IT-Risiken so früh wie möglich erkannt werden. Die CDC-Mitarbeiter:innen stehen bei Security-Incidents rund um die Uhr zur Verfügung. Im Bereich Incident Response übernimmt das CDC sicherheitsrelevante Analysetätigkeiten (Security Operations Center). Um die Sicherheitsvorfälle zu analysieren, werden unterschiedliche Methoden, Tools sowie primär ein forensischer Endpoint Agent verwendet. Sofern es technisch möglich ist, wird zudem eine Root-Cause-Analyse durchgeführt, um zukünftige Angriffe vonseiten des Einfallstors des Incidents zu verhindern.

CANCOM IT Disaster Recovery Architecture auf einen Blick.

Consulting

- Business-Impact-Analyse sowie nachfolgende Definition von Schadens- und Wiederanlaufklassen inkl. eines Zeitplans für den Wiederanlauf (Recovery Tier Map)
- Entwurf eines IT-Notfallplans und/oder einer IT-BCM-Richtlinie inkl. gemeinsamer Erarbeitung von Wiederherstellungsansätzen in verschiedenen Szenarien
- Gap-Analyse zu Industrie-Standards sowie Einbringen von Best-Practice-Ansätzen aus unseren Erfahrungen
- Design von Governance-Prozessen bis zur Durchführung von Wiederherstellungstests oder Planspielen (Tabletop Exercise)

Infrastracture

- Implementierung einer Business Continuity-/Disaster-Recovery-Lösung mit Fokus auf Ransomware
- Detailplanung der Zielarchitektur unter Berücksichtigung der Anforderungen aus der Consulting-Phase in einem Co-Creation Workshop
- Implementierung der dafür notwendigen Infrastruktur (Server, Storage, Lizenzen, Connectivity) On-Premises oder in der Cloud
- Periodische Restore-Tests und Erstellung von Recovery-Reports

Security

- Rund-um-die-Uhr-Unterstützung durch das CANCOM Cyber Defense Center
- Eigene Ansprechpartner:innen
- Kurze Reaktionszeiten
- Analyse von Windows-Systemen
- Linux-Live-Analyse
- Analyse sicherheitsrelevanter Log-Daten
- Analyse der Daten, Deklaration von erkannten sicherheitsrelevanten Bedrohungen

Vorteile und Mehrwerte

- **Reguläre Updates der IT-Disaster-Recovery-Basisinfrastruktur**
- **Halbjährlicher Reminder für abgestimmte Restore-Tests**
- **Keine Anschaffung von zusätzlicher Hardware notwendig**
- **Über das Emergency Response Service von CANCOM stehen Analyst:innen in den Pre-Incident- und Post-Incident-Phasen im Rahmen des definierten Service Level Agreements zur Verfügung**

CANCOM Austria: Österreichs führender ICT Serviceprovider & Digitalisierungspartner (bisher bekannt als Kapsch BusinessCom). Mit unserer Leidenschaft für Technologie und unserem zertifizierten Know-how für Collaboration, Netzwerk und IT-Technologie sind wir für Sie da als Consulter, Umsetzungspartner, Managed Service Provider und Digital Business Engineer. Wir entwickeln eigene Softwarelösungen und Plattformen auch für Ihre neuen Geschäftsmodelle. Als Digital Maker denken wir dabei immer end-to-end.

Besuchen Sie uns auf ↗ cancom.at

CANCOM Austria
Wienerbergstraße 53 // 1120 Wien // Österreich
T +43 50 822-0 // office@cancom.com // www.cancom.at

CANCOM