



Kompetent.
Zuverlässig.
Individuell.

Erste-Hilfe-Paket für Ransomware-Angriffe

Wir machen Sie fit für den Notfall!

Ransomware-Angriffe haben in den letzten Jahren stark zugenommen und verursachen erhebliche finanzielle und immaterielle Verluste durch Datenabfluss. Angesichts dieser Bedrohung haben viele Unternehmen Backup-Maßnahmen getroffen – **ein wichtiger erster Schritt**.

Doch dieser reicht nicht aus, um im Notfall die Schäden so gering wie möglich zu halten. Im Fall einer Erpressung können polizeiliche und forensische Ermittlungen angeordnet werden. Währenddessen können die betroffenen Unternehmen nicht mehr auf ihre Server und Netzwerk-

ressourcen zugreifen, da sie als digitaler Tatort untersucht werden. Das kann bis zu vier Monate dauern. Eine Parallelbeschaffung der notwendigen Infrastruktur ist wirtschaftlich meist nicht sinnvoll und aufgrund von Lieferengpässen oft nicht realisierbar. Somit ist eine Datenwiederherstellung auf dem üblichen Wege nicht mehr möglich.

Wir zeigen Ihnen konkret für Ihr Unternehmen, wie Sie bei solch einem Notfall Ihre Daten wiederherstellen und Ihre Geschäftsprozesse für Sie und Ihre Kunden wieder bereitstellen können – selbstständig, schnell und sicher.

Erste Hilfe: Disaster Recovery aus der Cloud

Mit unserem Service werden Sie befähigt, Ihren Geschäftsbetrieb nach einem Ransomware-Angriff souverän und zuverlässig wieder aufzunehmen. Diese Leistungen sind im Paket enthalten:



Mehrtägiger
Workshop



Schaffung der
technischen
Voraussetzungen



Probe der Notfall-
situation und Wie-
derherstellung der
IT-Services



Detaillierte
Handlungsanweisung



Abnahmetest/
Notfalltest

Seien Sie für Sicherheitsvorfälle bestens gewappnet –
Serviceverfügbarkeit auch im Falle polizeilicher Ermittlungen

Workshop-Ablauf

Erfassung der Bestandsressourcen

Ggf. Bereitstellung und Anbindung von Cloud-Speicher

Ggf. testweise Bereitstellung einer Cloud-Applikationsinfrastruktur

Kopie der Backup- und Disaster Recovery-Daten in Cloud bringen

Herstellung Disaster-Recovery-Konnektivität zwischen der Cloud- und On-Premise-Infrastruktur

Test der Wiederherstellung ausgewählter Systeme/Applikationen in der Cloud

Testbetrieb der Systeme/Applikationen in der Cloud bzw. hybrid

Auswertung der Ergebnisse

Erstellung eines Maßnahmenplans für den Notfall

Ihre Vorteile:



Speziell auf Ihr Unternehmen zugeschnitten



keine dauerhafte Cloud-Migration nötig



bestehende Cloud-Elemente vorteilhaft, aber nicht erforderlich



kein Shadow-Rechenzentrum nötig



Disaster Recovery unabhängig von Bandbreite



Ressourcenbuchung erst im Notfall



Nachweis eines stabilen Geschäftsbetriebes (Compliance)



Funktionalität und Wirksamkeit der Maßnahmen werden geprüft



Kernprozesse sind schnell wieder aktiv

Auszüge aus dem Bundeslagebild Cybercrime 2022 vom Bundeskriminalamt

- „Ransomware bleibt primäre Bedrohung für Unternehmen und öffentliche Einrichtungen.“
- „Von allen Malware-Arten hat Ransomware weiterhin das höchste Schadenspotential. Im Jahr 2022 wurde im Durchschnitt täglich mindestens ein deutsches Unternehmen Ziel eines Ransomware-Angriffs.“

Riskieren Sie nichts – sorgen Sie jetzt vor! Wir unterstützen Sie gern.