# Eine kleine Einführung in resiliente Datensicherung

**Wie lässt sich eigentlich die eigene Datenhaltung so gestalten, dass im Ernstfall keine wertvollen Informationen verloren gehen?**

**Aber was ist eigentlich der Ernstfall? Und was sind wertvolle Informationen? Welche Risiken gilt es zu betrachten und welche Maßnahmen kann man ergreifen um diese Risiken zu verringern oder gar ganz auszuschließen?**

**Dieser Vortrag gibt eine praxisorientierte Einführung in die Grundlagen resilienter Datensicherung. Ziel ist es, ein Verständnis dafür zu schaffen, wie man mit vertretbarem Aufwand eine zuverlässige und zukunftssichere Datensicherung plant und umsetzt.**

Nach einer kurzen Einführung, wozu man Datensicherung eigentlich braucht und was die üblichen Ursachen für einen Datenverlust sind, sehen wir uns im ersten Teil eine Reihe grundlegender Best Practices an.

Neben der 3-2-1 Methode werden die Themen Recovery-Point-Objective, Vorhaltezeiten, Validierung, Automatisierung und Katalogisierung behandelt. Wir werden im Detail sehen wieso jeder dieser Bereiche für sich genommen wichtig ist und welche Fallstricke sich in der Praxis ergeben können, wenn man hier nicht hinreichend geplant hat.

Im zweiten Teil gehen wir dann noch einen Schritt weiter und betrachten resiliente Datensicherung, also die Frage wie man eine Datensicherung so widerstandsfähig gestaltet, dass sie im Notfall auch wirklich rückgesichert werden kann.

Hier geht es neben der Erweiterung der 3-2-1 Methode zur 3-2-1-1-0 Methode insbesondere um Fragen wie Unveränderbarkeit, die Auswahl einer sicheren Off-Site, Recovery-Time-Objectives, Manipulationssicherheit und Zugriffskontrolle, aber auch um Pro und Contra von Verschlüsselung im Bezug auf die Verfügbarkeit einer Datensicherung oder den Stellenwert von Auditierung und Logging.

## Literaturquellen


**BSI IT-Grundschutz-Kompendium** *(Baustein CON.4 / OPS.1.1.2)*

**ENISA – Threat Landscape Reports (jährlich)**
*European Union Agency for Cybersecurity.*

**ISO/IEC 27031:2011**
*Guidelines for information and communication technology readiness for business continuity*

**ISO/IEC 27040:2015**
*Storage Security*

**ISO/*IEC* 22301:2019**
*Business Continuity Management Systems*

***SNIA – Data Protection Best Practices***
*Storage Networking Industry Association, aktueller Report.*

**NIST Special Publication 800-34 Rev. 1**
*Contingency Planning Guide for Federal Information Systems*

***NIST SP 800-184***
*Guide for Cybersecurity Event Recovery*