NIS2 & Wiederanlaufübungen: Wann Ihr Unternehmen wirklich „wiederherstellbar“ ist

Was ist eine Wiederanlaufübung?

Eine Wiederanlaufübung (Recovery Drill) ist ein **geplanter Test**, bei dem Sie simulieren, dass eine oder mehrere geschäftskritische Anwendungen ausgefallen oder kompromittiert sind – und diese Anwendungen aus Sicherungspunkten wieder in den Betrieb bringen.

Typischerweise umfasst die Übung:

- **Auslöser / Szenario:** z.B. Ransomware-Befall, korrupte Datenbank, Ausfall eines Rechenzentrums.
- **Wiederanlaufpfad:** von der Datenebene (Storage / Backups / Snapshots) über Datenbanken und Applikationslogik bis hin zu Zugriffsrechten und Schnittstellen.
- **Validierung:** prüfbare Kriterien, ob die Anwendung fachlich wieder nutzbar ist (z.B. Testfälle aus dem Fachbereich).
- **Metriken:** insbesondere **RTO** (Zeit bis zur Betriebsbereitschaft), **RPO** (maximaler Datenverlust) sowie **Wiederherstellungsleistung in TB/h**.

Ziel ist nicht nur ein „technischer Restore“, sondern der **nachweisbare Wiederanlauf eines Geschäftsprozesses**.

Warum fordert NIS2 Wiederanlaufübungen?

NIS2 macht **Verfügbarkeit, Integrität und Wiederherstellbarkeit** zu zentralen Schutzzielen. In der deutschen Umsetzung (NIS2UmsuCG) sind u.a. folgende Punkte relevant:

- Unternehmen müssen **geeignete technische und organisatorische Maßnahmen** zum Risikomanagement umsetzen (u.a. Backup, Wiederherstellung, Krisenmanagement).
- Sie sollen **regelmäßig testen**, ob diese Maßnahmen wirksam sind – dazu gehören Wiederanlaufübungen mit aussagekräftigen Kennzahlen.
- Für wichtige und besonders wichtige Einrichtungen entstehen **Nachweis-**

und Dokumentationspflichten gegenüber Aufsichtsbehörden.

- Haftbarkeit für Geschäftsführer mit einbauen – Nach der Umsetzung in nationales Recht (z.B. § 38 BSIG-E in Deutschland) haftet die Geschäftsleitung für die Überwachung und Umsetzung der Cybersicherheitsmaßnahmen.

Praktisch bedeutet das:
Ohne geübte, dokumentierte Wiederanlaufübungen mit klaren Metriken wird es schwer, gegenüber Prüfern und Aufsicht glaubhaft von „NIS2-konformer Wiederherstellbarkeit“ zu sprechen.

Wann gilt eine Wiederanlaufübung als erfolgreich?

Eine Übung ist mehr als „grün“, wenn ein Restore technisch durchläuft. Sie sollte mindestens folgende Kriterien erfüllen:

1. **RTO/RPO erreicht oder bewusst verfehlt**
   - Die Übung zeigt, ob definierte Ziele (z.B. **RTO ≤ 24 Stunden** für bestimmte Anwendungen) erreichbar sind.
   - Abweichungen werden dokumentiert und in Maßnahmen überführt.

2. **Fachliche Nutzbarkeit wiederhergestellt**
   - Anwendung ist wieder erreichbar („online“).
   - Fachbereich bestätigt, dass alle zentralen Funktionen wie vorgesehen arbeiten (z.B. Buchungen, Laborbefunde, Leitsysteme).
   - Der zugehörige Geschäftsprozess ist wieder vollständig und in gleicher Qualität wie vor dem Incident nutzbar.

3. **„Sauberer“ Wiederanlauf**
   - Es gibt Indizien, dass aus **vertrauenswürdigen, unveränderlichen Sicherungspunkten** wiederhergestellt wurde (z.B. Snapshots/Backups mit Immutability auf der Storage-Ebene).
   - Es liegen keine Hinweise auf erneute Kompromittierung vor (z.B. durch begleitende Security-Checks).

4. **Messwerte dokumentiert**
   - Wiederherstellte Datenmenge (z.B. in TB) + RPO / RTO erreicht?
   - Dauer vom Start der Wiederherstellung bis zur Freigabe durch den Fachbereich (RTO).

- Korrekten RPO erreicht?
- Effektive **Wiederherstellungsleistung (TB/h)**, idealerweise pro Stufe (Storage, DB, App).

5. **Lernkurve sichtbar**
    - Identifizierte Schwachstellen (z.B. fehlende Runbooks, zu geringe Bandbreite, unklare Rechtevergabe).
    - Konkrete Maßnahmen mit Verantwortlichen und Fristen.

Welche Rollen sollten beteiligt sein?

Eine belastbare Wiederanlaufübung ist ein **gemeinsames Projekt** von Security, IT-Betrieb und Fachbereichen:

- Geschäftsführung ist immer mit involviert, ohne GF / C-Level Awareness wird es nicht ernst genommen, da kann man noch etwas ausformulieren zu.

- **CISO / Security Owner**
    - Verantwortlich für Einbettung in das **NIS2-Risikomanagement**, Vorgaben zu Szenarien und Akzeptanzkriterien („Was ist ein tolerierbarer Rest-Risiko-Level?“).
    - Abnahme der Übung aus Sicht Informationssicherheit und Bericht an Geschäftsleitung/Aufsicht.

- **IT-Leitung / Head of Infrastructure & Storage**
    - Verantwortlich für Architektur, Kapazitäten und **Wiederanlaufpfad** (Storage, Netzwerk, Compute).
    - Stellt sicher, dass die Storage-Ebene RTO/RPO-Ziele überhaupt technisch leisten kann (z.B. Restore-Durchsatz, Snapshots, Replikation).

- **BCM/DR-Verantwortliche**
    - Koordination der Übung, Definition von Scope, Zeitfenster, Schnittstellen zu Krisenstab/Kommunikation.
    - Auswertung der Ergebnisse und Pflege der Runbooks.

- **Applikations- und Datenbank-Owner**
    - Definition fachlicher Testfälle.
    - Validierung, ob die Anwendung nach dem Wiederanlauf tatsächlich arbeitsfähig ist.

- **Security Operations (SIEM/SOC)**
    - Begleitende Überwachung (z.B. ungewöhnliche Aktivitäten während Übung).
    - Einbezug der Storage- und Backup-Events in Use-Cases (z.B. Löschung von Snapshots, Policy-Änderungen).

Was muss dokumentiert werden?

Für NIS2-Audits und interne Governance sollte jede Übung mindestens folgende Unterlagen erzeugen:

1. **Übungssteckbrief**
    - Datum, Dauer, beteiligte Systeme/Anwendungen, Scope (z.B. nur Testumgebung vs. produktionsnah).
    - Zielsetzung (z.B. „RTO ≤ 24h unter Beweis stellen“ oder „Pilot für Container-Workloads“).

2. **Szenario und Annahmen**
    - Art des Vorfalls (Ransomware, logische Korruption, Standortausfall).
    - Annahmen zu verfügbaren Ressourcen (z.B. Personal, Netzbandbreite, Offsite-Kopien).

3. **Technischer Ablauf**
    - Genutzte Sicherungspunkte (z.B. Snapshots/Backups auf der Storage-Ebene, Replikationsziele).
    - Schritte von Storage-Restore über DB-Recovery bis zum Start der Anwendung.

4. **Metriken und Ergebnisse**
    - Wiederhergestellte Datenmenge (TB).
    - RTO (Start – Freigabe), RPO (Datenstand).

- Beobachtete Wiederherstellungsleistung (TB/h) und Engpässe.

5. **Bewertung und Maßnahmenplan**
    - Ampelbewertung pro Aspekt (z.B. Storage, Netzwerk, DB, Applikation, Organisation).
    - Konkrete Verbesserungsmaßnahmen mit Verantwortlichen und Terminen.

Die Storage-Plattform spielt hier eine besondere Rolle: Sie liefert die **Messwerte und Sicherungspunkte**, aus denen die Anwendung überhaupt wieder entstehen kann – und damit wesentliche Evidenz für NIS2-Prüfungen.

Wie oft sollte geübt werden?

NIS2 schreibt keine fixe Frequenz pro Anwendung vor, erwartet aber ein **angemessenes Risikomanagement**. In der Praxis haben sich bewährt:

- **Mindestens 1× jährlich** eine umfassende Übung für die wichtigsten Services (z.B. Top-5-Anwendungen).
- **Zusätzliche, kleinere Übungen** (Teilübungen) nach wesentlichen Änderungen:
    - Neue Speicher- oder Backup-Plattform,
    - größere Architekturänderungen,
    - neue geschäftskritische Anwendungen,
    - nach relevanten Security-Incidents.

Wichtig ist weniger eine „perfekte“ Großübung, sondern ein **kontinuierlicher Verbesserungsprozess**, der dokumentiert, wie sich Ihre Wiederherstellbarkeit entwickelt – und welche Rolle die Storage-Ebene dabei spielt.

Fazit

Für das CISO Office, IT-Leitung und Entscheider:innen sind Wiederanlaufübungen unter NIS2 keine „nice-to-have“-Techniktests, sondern ein **zentrales Governance-Instrument**:

- Sie belegen, dass Wiederherstellbarkeit nicht nur auf dem Papier existiert,

sondern **geübt und messbar** ist.
- Sie machen sichtbar, ob Architektur, Prozesse und Rollen zur **Storage-Ebene** und darüber hinaus zusammenpassen.
- Sie liefern die Evidenzen, die NIS2-Prüfende und Aufsichten künftig erwarten werden.

Wer frühzeitig strukturiert übt, schafft sich nicht nur Rechtssicherheit – sondern vor allem die Sicherheit, im Ernstfall **schnell, sauber und nachvollziehbar** wieder an den Start zu kommen.Inhalte hier hinzufügen