cycura

Handlungsfähig im Ernstfall

Der Azure Emergency Tenant – warum Backup allein nicht reicht und wie Sie kontrollierte Wiederherstellung sicherstellen

Die Realität: Die meisten Notfallpläne funktionieren nicht, wenn der Tenant kompromittiert ist

Viele Unternehmen verlassen sich auf Backup-Systeme und Papierpläne. Doch wenn Exchange, Teams oder Entra ID kompromittiert sind, fehlt die technische Grundlage für Kommunikation und Wiederherstellung. Die Folge: Tage der Handlungsunfähigkeit, während der Schaden wächst.

Was Sie in diesem Guide erwartet

- Die 4 kritischen Lücken in herkömmlichen Notfallkonzepten
- Warum Backup keine Handlungsfähigkeit garantiert
- Das Framework für einen Azure Emergency Tenant
- Ein Selbstcheck: Können Sie im Ernstfall noch kommunizieren?

cycura

Die 4 Fragen, die Sie sich heute beantworten müssen

1. Wie kommunizieren wir, wenn Exchange, Teams oder Entra ID kompromittiert sind?

Wenn Ihre primären Kommunikationskanäle nicht verfügbar oder nicht vertrauenswürdig sind, wie koordinieren Sie den Krisenstab?

2. Wo melden sich Administratoren an, wenn der Produktiv-Tenant nicht mehr vertrauenswürdig ist?

Wenn Identitäten kompromittiert sind oder der Tenant gesperrt wird, haben Sie keine administrative Zugriffsbasis mehr.

3. Wie stellen wir Identitäten, Zugriff und Steuerung wieder her – ohne Abhängigkeiten zum kompromittierten System?

Backup-Daten nützen nichts, wenn Sie keine saubere Umgebung haben, um sie wiederherzustellen.

4. Wer entscheidet was – und auf welcher technischen Grundlage?

Ohne vordefinierte, getestete Prozesse entscheiden Sie unter Druck improvisiert – oft mit veralteten oder unvollständigen Informationen.

cycura

1

Die Kommunikationslücke

DIE LÜCKE

Exchange Online und Teams sind kompromittiert oder nicht verfügbar. Die regulären Kommunikationskanäle fallen aus – genau wenn Sie sie am dringendsten brauchen. Externe E-Mail-Accounts oder Messenger sind unsicher und nicht compliant.

DAS KONKRETE RISIKO

Der Krisenstab kann sich nicht koordinieren, Entscheidungen verzögern sich um Stunden oder Tage. Externe Partner und Kunden erreichen Sie nicht. Die öffentliche Wahrnehmung entgleitet Ihnen, während Sie technisch handlungsunfähig sind.

WAS WIR IN ASSESSMENTS FINDEN

- Keine definierte alternative Kommunikationsplattform für Katastrophenfälle
- Abhängigkeit von kompromittierten Identitäten für Notfallkommunikation
- Fehlende Trennung zwischen Produktiv- und Notfallkommunikation
- Keine vorab festgelegten Kommunikationswege für externe Stakeholder

PRÜFPFAD

Notfallplan → Kommunikationsmatrix → Technische Basis der Notfallkanäle → Unabhängigkeit vom Produktiv-Tenant prüfen

cycura

2

Die Identitätsfalle

DIE LÜCKE

Wenn Entra ID kompromittiert ist oder der Tenant gesperrt wird, verlieren Sie den administrativen Zugriff. Globale Administratoren können sich nicht anmelden, Conditional Access blockiert legitime Zugriffe, MFA-Systeme sind nicht erreichbar.

DAS KONKRETE RISIKO

Sie haben keine technische Möglichkeit, den Wiederherstellungsprozess zu starten oder zu steuern. Selbst wenn Sie saubere Backups haben, fehlt die saubere Identitätsbasis, um darauf zuzugreifen. Die Wiederherstellung verzögert sich um Tage, weil Sie erst eine vertrauenswürdige administrative Umgebung aufbauen müssen.

WAS WIR IN ASSESSMENTS FINDEN

- Keine entkoppelten Notfall-Identitäten außerhalb des Produktiv-Tenants
- Alle Admin-Accounts im gleichen Entra ID ohne Air-Gap
- Fehlende Hardware-Token oder Break-Glass-Accounts außerhalb der Cloud
- Keine dokumentierten, getesteten Zugriffspfade für den Ernstfall

PRÜFPFAD

Entra ID → Notfall-Admin-Accounts → Abhängigkeitsprüfung → Break-Glass-Verfahren → Alternative Authentifizierungsbasis

cycura

3

Die Wiederherstellungs-Illusion

DIE LÜCKE

Sie haben Backups Ihrer Daten – aber keine entkoppelte, saubere Umgebung, um diese wiederherzustellen. Ein Restore in den kompromittierten Tenant bringt nichts (Ransomware liegt im Backup mit). Ein Restore in eine neue Umgebung dauert Tage, wenn diese erst noch aufgebaut werden muss.

DAS KONKRETE RISIKO

Sie verlieren wertvolle Zeit beim Aufbau einer sauberen Infrastruktur, während das Geschäft stillsteht. Die Wiederherstellung vermischt sich mit dem Wiederaufbau des kompromittierten Systems, was zu Re-Infektionen führt. Kritische Steuerungskomponenten (AD, DNS, PKI) fehlen oder sind ebenfalls kompromittiert.

WAS WIR IN ASSESSMENTS FINDEN

- Backup-Strategien ohne Zielumgebung für den Restore
- Fehlende Trennung zwischen Wiederherstellung und Wiederaufbau
- Keine vorab definierte saubere Azure-Umgebung für Notfallfälle
- Unklare RTO-Definitionen für Steuerungskomponenten vs. Anwendungsdaten

PRÜFPFAD

Backup-Konzept → Zielumgebung für Restore → Trennung kompromittiert/sauber → Infrastructure as Code für Notfallumgebung

cycura

4

Die Prozess-Lücke

DIE LÜCKE

Notfallpläne existieren auf Papier, wurden aber nie unter realistischen Bedingungen getestet. Die technischen Abläufe sind nicht dokumentiert, die Verantwortlichkeiten unklar. Unter Druck werden improvisiert Entscheidungen getroffen, die den Schaden vergrößern.

DAS KONKRETE RISIKO

Während des Incidents entstehen Fehler durch Unwissenheit: Falsche Reihenfolge der Wiederherstellung, vergessene Abhängigkeiten, unsichere Kommunikationswege. Der Recovery-Prozess verlängert sich um Faktor 3-5 gegenüber einem getesteten Verfahren. Mitarbeiter sind überfordert, da sie die Notfallumgebung nie gesehen haben.

WAS WIR IN ASSESSMENTS FINDEN

- DR-Pläne, die zuletzt vor 12+ Monaten aktualisiert wurden
- Keine Fire-Drills oder Tabletop-Übungen mit der Notfallumgebung
- Fehlende Infrastructure as Code (IaC) Dokumentation
- Unklare Eskalationswege wenn primäre Entscheider nicht erreichbar sind

PRÜFPFAD

Notfallplan → Letzter Testdurchlauf → Dokumentationsstand → IaC-Vollständigkeit → Schulungsnachweise

cycura

Die Lösung: Ein entkoppelter Azure Emergency Tenant

Der Azure Emergency Tenant ist keine Backup-Software und kein Papierplan. Es ist eine technisch und organisatorisch entkoppelte Notfallumgebung innerhalb von Microsoft Azure, die Handlungsfähigkeit sicherstellt – auch wenn der Produktiv-Tenant kompromittiert ist.

Was der Azure Emergency Tenant leistet

Entkoppelte Notfallumgebung: Separater Azure-/Entra-Tenant ohne technische Abhängigkeiten zum Produktivbetrieb. Kein lateraler Zugriff aus kompromittierten Umgebungen.

Sofort verfügbare Kommunikation: Teams und Exchange für definierte Rollen (Krisenstab, IT, Security, Management), nutzbar unabhängig vom Zustand des Haupttenants.

Kontrollierte Wiederherstellung: Sauberer Startpunkt für Wiederherstellung kritischer Identitäten und Steuerungskomponenten ohne Vermischung mit kompromittierten Strukturen.

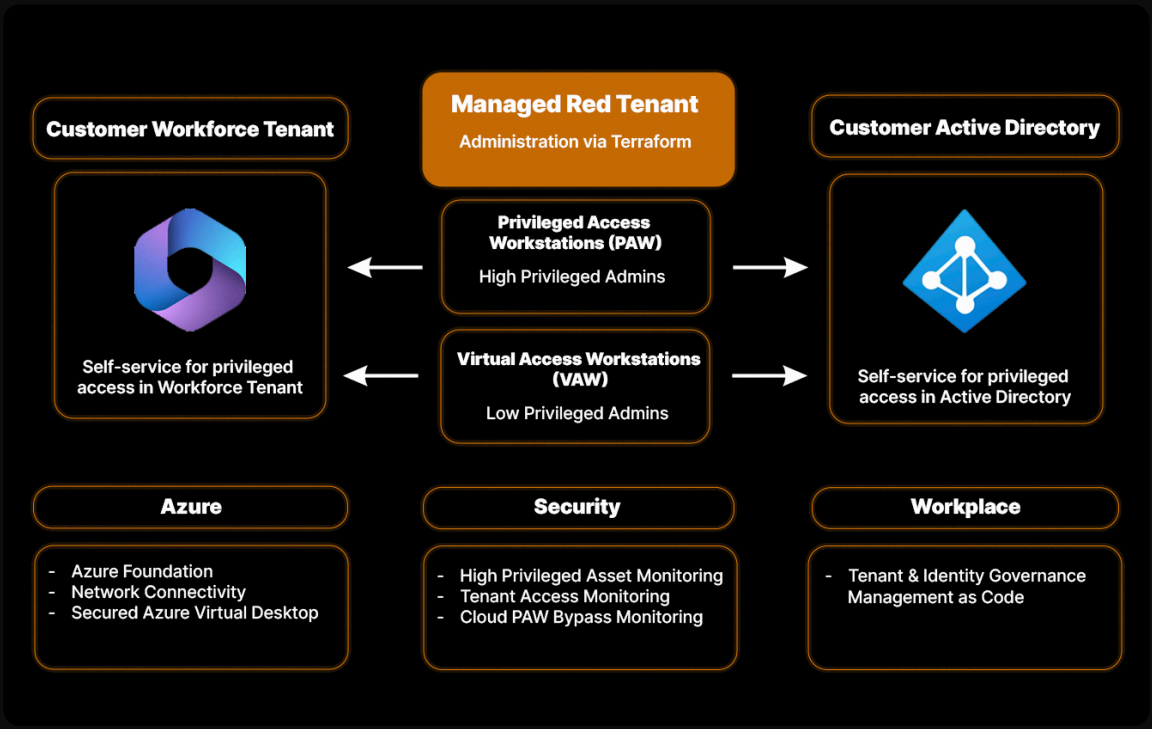
Infrastructure as Code: Vordefinierte, versionierte und getestete Notfallprozesse. Reproduzierbarkeit statt Improvisation.

Regelmäßige Validierung: Monatliche Fire-Drills und Wiederherstellungstests zur Validierung von Datenkonsistenz und Abläufen.

cycura

Wie der Azure Emergency Tenant technisch funktioniert

Der Emergency Tenant ist ein vollständig separater Microsoft 365 Tenant mit eigener Entra ID, eigenen Domains und keiner technischen Verbindung zum Produktivsystem.



Die Architektur im Überblick

- **Eigener Entra ID Tenant:** Separate Identitätsverwaltung ohne Vertrauensstellung zum Produktiv-Tenant
- **Eigene Domains:** Notfall-Domains (z.B. company-emergency.de) unabhängig von den Produktiv-Domains
- **Eigene Azure AD:** Keine Synchronisation, keine Federation, kein lateral movement möglich
- **Eigene Exchange/Teams:** Kommunikationsinfrastruktur, die auch bei Totalausfall des Hauptsystems läuft

cycura

Warum die Trennung so wichtig ist

Air-Gap Prinzip

- Kein lateraler Zugriff aus dem kompromittierten Produktiv-Tenant
- Keine gemeinsamen Administratoren ohne explizite Notfall-Accounts
- Keine Abhängigkeit von der Verfügbarkeit des Haupt-Entra ID
- Sauberer Air-Gap für forensische Untersuchungen

Die drei Säulen der Trennung

- **Organisatorisch:** Andere Admins, andere Prozesse, andere Verantwortlichkeiten
- **Technisch:** Keine Vertrauensstellungen, keine Federation, keine gemeinsamen Identitäten
- **Netzwerk:** Separate Domains, separate DNS, separate VPN-Zugänge

cycura

Infrastructure as Code: Der Emergency Tenant als Code

Die gesamte Emergency Tenant Konfiguration ist als Code dokumentiert – nicht als PDF, nicht als Word-Dokument, sondern als ausführbare Skripte.

Vorteile von Infrastructure as Code:

- **Reproduzierbarkeit:** Der Tenant kann jederzeit identisch neu aufgesetzt werden
- **Versionierung:** Alle Änderungen sind in Git nachvollziehbar
- **Dokumentation:** Der Code ist die Dokumentation – keine veralteten Handbücher
- **Automatisierung:** Deployment läuft vollständig automatisiert ab
- **Review-Prozess:** Änderungen werden vor dem Deployment geprüft

Was wird als Code verwaltet?

- **Entra ID Konfiguration:** Benutzer, Gruppen, Rollen, Conditional Access Policies
- **Exchange Online:** Mailboxes, Transportregeln, Retention Policies
- **Teams Konfiguration:** Teams, Kanäle, Berechtigungen, Meeting Policies
- **Security-Einstellungen:** MFA, Identity Protection, PIM, App-Registrierungen
- **Netzwerkkonfiguration:** DNS, Firewall-Regeln, VPN-Integration

Verwendete Tools

- **Terraform:** Für Azure Ressourcen und Infrastruktur
- **Bicep/ARM:** Für Microsoft 365 spezifische Konfigurationen
- **PowerShell DSC:** Für Windows-spezifische Einstellungen
- **Git:** Für Versionierung und Change Tracking

cycura

Was der Azure Emergency Tenant bewusst NICHT ist

Kein klassisches Backup-Produkt

Er ersetzt nicht Ihre Backup-Lösung, sondern ergänzt sie durch eine saubere Zielumgebung und Wiederherstellungsprozesse.

Kein DR-Konzept auf Papier

Keine theoretischen Pläne, sondern eine betriebsfähige, regelmäßig getestete technische Umgebung.

Kein Ersatz für Incident Response

Er stellt die technische Grundlage für IR-Maßnahmen bereit, ersetzt aber nicht das IR-Team oder dessen Prozesse.

Kein reines Infrastrukturprojekt

Technik allein reicht nicht – Organisation, Prozesse und regelmäßige Tests sind integraler Bestandteil.

cycura

Der Notfallvorsorge-Reifegrad-Check

Stufe	Beschreibung
1 Ad-hoc	Kein Notfallplan oder nur theoretische Dokumentation. „Wir haben ein Backup."
2 Definiert	Backup existiert, aber keine entkoppelte Wiederherstellungsumgebung. RTO in Tagen.
3 Gesteuert	Emergency Tenant existiert, aber unregelmäßig getestet. Prozesse sind dokumentiert, aber nicht automatisiert.
4 Optimierend	Regelmäßige Fire-Drills (monatlich), IaC-vollständig, klare RTO von Stunden für kritische Funktionen.
5 Exzellent	Vollständige Automation, integrierte Notfallkommunikation, dokumentierte RTO von <4 Stunden für Steuerungskomponenten, jährliche externe Audits.

> **Die gute Nachricht:** Die meisten Unternehmen befinden sich auf Stufe 1 oder 2 – und können mit gezielten Maßnahmen innerhalb von 3-6 Monaten Stufe 3 erreichen. Der Sprung zu Stufe 4 ist der kritische Schritt zur messbaren Handlungsfähigkeit.

Wo stehen Sie? – 5 Fragen zum Selbstcheck (Ja/Nein)

1. Können Sie kommunizieren, wenn Exchange und Teams im Produktiv-Tenant ausfallen?
2. Haben Administratoren einen Zugriffspfad, der unabhängig vom Produktiv-Entra ID funktioniert?
3. Gibt es eine technisch saubere Umgebung für die Wiederherstellung ohne Abhängigkeiten zum kompromittierten System?
4. Wurden Ihre Notfall-Wiederherstellungsprozesse in den letzten 6 Monaten praktisch getestet?
5. Können Sie kritische Steuerungskomponenten innerhalb von 24 Stunden wiederherstellen?

cycura

Der 12-Punkte Risiko-Check (bei bestehendem Microsoft-Tenant)

Beantworten Sie die folgenden Fragen mit Ja oder Nein. Jedes „Nein" ist ein potenzielles Risiko.

Kategorie: Notfallkommunikation

1. Gibt es eine Kommunikationsplattform (Teams/Exchange), die unabhängig vom Produktiv-Tenant funktioniert?
2. Sind alle Krisenstab-Mitglieder mit Notfall-Identitäten in dieser Umgebung eingerichtet?
3. Ist der Zugang zu dieser Kommunikationsumgebung auch bei Totalausfall des Haupt-Tenants gewährleistet?

Kategorie: Administrative Kontrolle

4. Existieren Break-Glass-Accounts außerhalb des Produktiv-Entra ID?
5. Haben Sie Hardware-Token oder alternative MFA-Methoden für den Emergency-Zugriff?
6. Können Sie administrative Aktionen ausführen, ohne auf den kompromittierten Tenant zugreifen zu müssen?

Kategorie: Wiederherstellung & Infrastruktur

7. Existiert ein separater Azure-Tenant ausschließlich für Notfallzwecke?
8. Ist die Notfallumgebung durch IaC (Infrastructure as Code) vollständig dokumentiert und reproduzierbar?

cycura

Der 12-Punkte Risiko-Check (Fortsetzung)

Kategorie: Prozesse & Testung

10 Wurden die Wiederherstellungsprozesse für kritische Systeme in den letzten 3 Monaten getestet?

11 Gibt es dokumentierte RTO-Ziele (Recovery Time Objective) für Steuerungskomponenten?

12 Sind die Verantwortlichkeiten im Notfall klar definiert und den Beteiligten bekannt?

Auswertung

Nein-Antworten	Risikostufe	Empfohlene Maßnahmen
0-2	Niedrig	Kontinuierliche Optimierung, regelmäßige Tests
3-5	Mittel	Lücken schließen, Emergency Tenant konzipieren
6-9	Hoch	Sofortige Planung eines Emergency Tenants erforderlich
10-12	Kritisch	Keine belastbare Notfallvorsorge, dringender Handlungsbedarf

Mehr als 3x „Nein"? Ihre Notfallvorsorge hat signifikante Lücken. Wir helfen Ihnen, einen Azure Emergency Tenant systematisch aufzubauen. **www.cycura.de/termin**

cycura

Impressum

cycura GmbH

Ihr Spezialist für Microsoft-Security

Kontakt:

E-Mail: info@cycura.de

Web: www.cycura.de

Handelsregister: Amtsgericht Göttingen HRB 206706

USt-IdNr.: DE354593485

Bereit für den Ernstfall?www.cycura.de/termin