
OVERLAND TANDBERG
NetJapan
Ein IT-Notfall während Sie auf Urlaub sind – Albtraum oder Realität?
Der schlimmste Albtraum wird schnell zur Realität – im Urlaub erhalten Sie 10 Nachrichten auf Ihrer Mailbox von Ihrem Chef. Er erwartet dringend Ihren Rückruf wegen eines IT-Notfalls "Serverausfall und die Kollegen können nicht mehr arbeiten". Man benötigt dringend Ihre Hilfe für eine "prompte Wiederherstellung der Backups!" Aber was ist mit dem Mojito, den Sie gerade bestellt haben?
Get it back

Jeder verdient eine Auszeit von der Arbeit. Kleinere und mittlere Unternehmen verfügen oft nur über einen IT-Experten, der sich um die IT-Infrastruktur oder auch nur um die Backups kümmert. Wie stellen Sie, als IT-Profi oder Verantwortlicher für die Backups sicher, dass sich Ihr wohlverdienter Urlaub, im IT-Katastrophenfall oder im Fall einer Cyber-Attacke, nicht in einem Albtraum verwandelt?

Nicht zutreffend für Sie? Sind Sie überzeugt, dass Ihr Unternehmen sicher und auf jeden IT-Notfall vorbereitet ist, selbst wenn Sie tausende Kilometer entfernt sind? Es gibt zu viele Fälle, bei denen es schon zu spät war! Welche Maßnahmen sind notwendig, damit IT-Fachleute beruhigt auf Urlaub gehen und die Auswirkungen von Katastrophen auf ein Minimum begrenzt sind?

Checkliste für Ihr Backup bevor Sie auf Urlaub gehen

Prüfen Sie Ihre Backup-Aufgaben auf volle Funktionstüchtigkeit.

- ○ Aufbewahrungsrichtlinie sollte aktiviert sein
- ○ Backup-Datei Größe prüfen
- ○ Verfügbaren Speicherplatz prüfen
- ○ Vergewissern Sie sich, dass Ihre Einstellungen zur Fehlerbenachrichtigung aktiv sind und an eine gültige E-Mail gesendet werden..

Bewahren Sie mindestens eine Kopie Ihrer Daten Off-Site auf, so erhöhen Sie den Schutz bei lokalen Katastrophen oder Cyber-Attacken. Wir empfehlen die Verwendung der **Speichermedienrotation** und /oder die **3-2-1 Backup Tipps.**

Führen Sie vor Ihrem Urlaub einen letzten Test zur Wiederherstellung aus.

Führen Sie vor Ihrem Urlaub einen Notfall-Failover-Test via Fernzugriff aus..

Erstellen Sie einen genauen Disaster-Recovery-Plan und geben Sie den Speicherort der Sicherungskopie an, die Off-Site aufbewahrt wird. Halten Sie Ihre Notizen

- ○ Im elektronischen Format
- ○ Im Papierformat
- ○ Als On-Site und Off-Site Kopie
- ○ Zugänglich und bekannt für mehrere Personen im Unternehmen
- ○ Fügen Sie Ihrem Notfallplan auch einen Urlaubs-/ Krankheits-Backup- und Wiederherstellungsplan hinzu und bestimmen Sie die Verantwortlichkeiten.
- ○ Notieren Sie den gesamten Backup-Vorgang einschließlich Backup-Aufgaben und die Handhabung der Wechseldatenträger für den Off-Site Schutz.

Maßnahmen für Ihre Backups bevor Sie auf Urlaub gehen

Die folgenden Maßnahmen basieren auf Problemen, die andere IT-Profis bereits erlebt haben. Sorgen Sie dafür, dass Ihnen so etwas nicht passiert! Seien Sie für den IT-Notfall gerüstet!

Backup und Disaster Recovery Plan erstellen

Erstellen Sie Ihren Backup- und DR Plan und kommunizieren Sie den Plan an Ihre Kollegen, Ihre Administration und stellen Sie die Notizen auch in gedruckter Form zur Verfügung. 40 % der Unternehmen haben keinen dokumentierten DR Plan!

Umsetzung der 3-2-1 Backup Strategie

Für einen umfassenden Schutz bei IT-Katastrophen empfehlen wir Unternehmen die 3-2-1 Backup-Strategie, mit einem Speichergerät als primäres Backup-Ziel und einem anderen als sekundäres Backup-Ziel. Fällt eines der beiden Speichergeräte aus, kann auf das verbleibende Speichergerät für die Wiederherstellung Ihrer Daten und Systeme zurückgegriffen werden. Zusätzlich sollte eine dritte Kopie der Backup-Ketten auf einem Wechseldatenträger gespeichert werden.

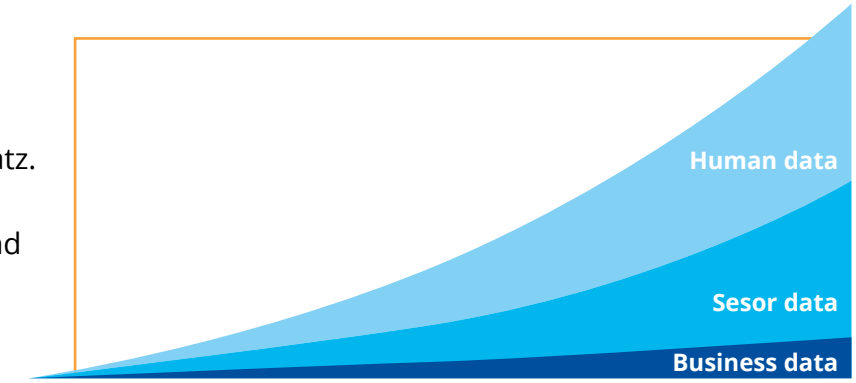
Simulation eines Extremfalls

Integrieren Sie in Ihren DR Plan das schlimmste Notfall-Szenario, dass Sie sich vorstellen können. Beispiel: Eine Cyber-Attacke verschlüsselt Ihre Daten und Systeme, während Sie auf Urlaub sind und Ihre Vertretung ist plötzlich krank. Es ist nicht sehr wahrscheinlich, dass so ein Fall eintritt, aber man weiß nie. Es ist immer gut die Kontrolle zu behalten!

Lokale Backups jederzeit bereit

Überprüfung freier Speicherkapazitäten

Prüfen Sie den noch verfügbaren Speicherplatz. Das Datenvolumen wächst exponentiell bei einer Rate von x50 von Jahr zu Jahr. Kleine und mittlere Unternehmen prüfen oftmals nicht ihre Wachstumsrate bei Daten und merken zu spät, dass ihre Speichermedien bereits voll sind.



Aufbewahrungsrichtlinie prüfen

Stellen Sie sicher, dass alte Backups gelöscht werden und Platz schaffen für neue Backup-Dateien. Diese Richtlinie ist meist als Option verfügbar und muss erst aktiviert werden, da sie nicht standardmäßig aktiviert ist. Berechnen Sie, wie viele Backup-Sets (vollständige Sicherung inklusive inkrementeller Sicherungen) Sie behalten können, damit diese mit der Kapazität Ihres Backup-Speichers übereinstimmen.

Fehlerbenachrichtigungen dürfen nicht ignoriert werden

Eine Benachrichtigung sollte nur im Falle eines Fehlers erfolgen, andernfalls werden die Ereigniseinträge überladen. Wird ein Backup auf Grund fehlender Speicherkapazitäten nicht erstellt, so ist das Problem schnell und einfach zu lösen.

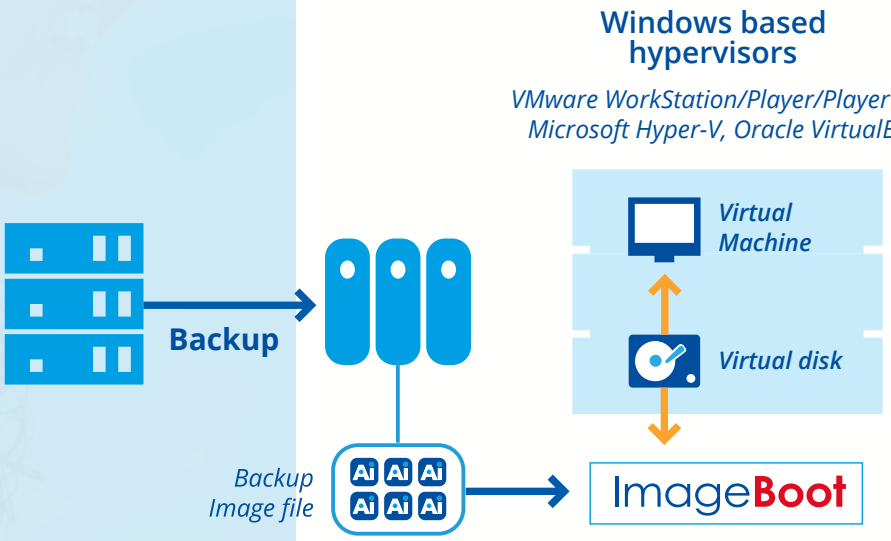
Prüfen Sie Ihre Backup-Dateien!

Warum ist eine Überprüfung der Backup-Dateien notwendig?

Mit der Zeit kann ein Schaden am Speichergerät auftreten, z.B. beschädigte Hardware oder fehlerhafte Blöcke, und verursacht Datenverlust oder korrumpiert inkrementelle Dateien ohne Vorankündigung. Ist ein inkrementelles Backup in der Mitte der Backup-Kette betroffen, können Sie keine der nachfolgenden Dateien wiederherstellen, selbst wenn ein erfolgreiches Backup mit Ihrer Software erstellt wurde.

Backup-Verifizierung ist gut, noch besser ist das Prüfen der Backup-Wiederherstellung

Einige Backup-Unternehmen bieten Verifizierungstests, um die gesamte Backup-Kette zu überprüfen. Diese Funktion kontrolliert, ob jeder Block der Sicherungsdatei lesbar ist. Der Vorgang dauert oft sehr lange und viele Firmen nutzen diese Option nicht, der Test ist jedoch sicherer als eine einfache MD5 -Verifizierung.



Doch auch Verifizierungsprozesse garantieren nicht, dass Sie Ihre Backups wiederherstellen können, falls eine Katastrophe eintritt. Warum? Die Verifizierung prüft nur, ob Ihre Backups lesbar sind jedoch nicht den Blockinhalt – wie zum Beispiel eine defekte Partitionstabelle – da sind MD5 und Verifizierungsprozesse anwendbar, aber Sie werden trotz erfolgreicher Tests die wiederhergestellte Maschine nicht starten können. (Sie können versuchen die beschädigte Partition zu reparieren, dies erhöht jedoch Ihre Ausfallzeiten).

Virtualisierungstechnologien wie ImageBoot, die in NetJapan ActiveImage Protector Backup & Disaster Recovery Lösungen (für Windows und Linux) enthalten sind, ermöglichen einfache und schnelle Backup-Tests und sind für jede Organisation zugänglich. IT-Profis starten Backup-Dateien (von physischen oder virtuellen Maschinen) in virtuellen Umgebungen in weniger als 5 Minuten.

Vorteile eines Backup "Wiederherstellbarkeitstest" versus Backup Verifizierung

- **Zuverlässigkeit:** Prüfen und überzeugen Sie sich selbst, dass die ausgewählten Backup-Dateien booten und somit die Kette bis zu diesem Punkt sicher und zuverlässig ist.
- **Geschwindigkeit:** Verkürzung der Backup-Testzeit auf ein paar Minuten.
- **Häufigkeit:** Da dieser Vorgang nur wenige Minuten in Anspruch nimmt, verifizieren Sie Ihre Backup-Kette einfach jede Woche oder noch öfter.

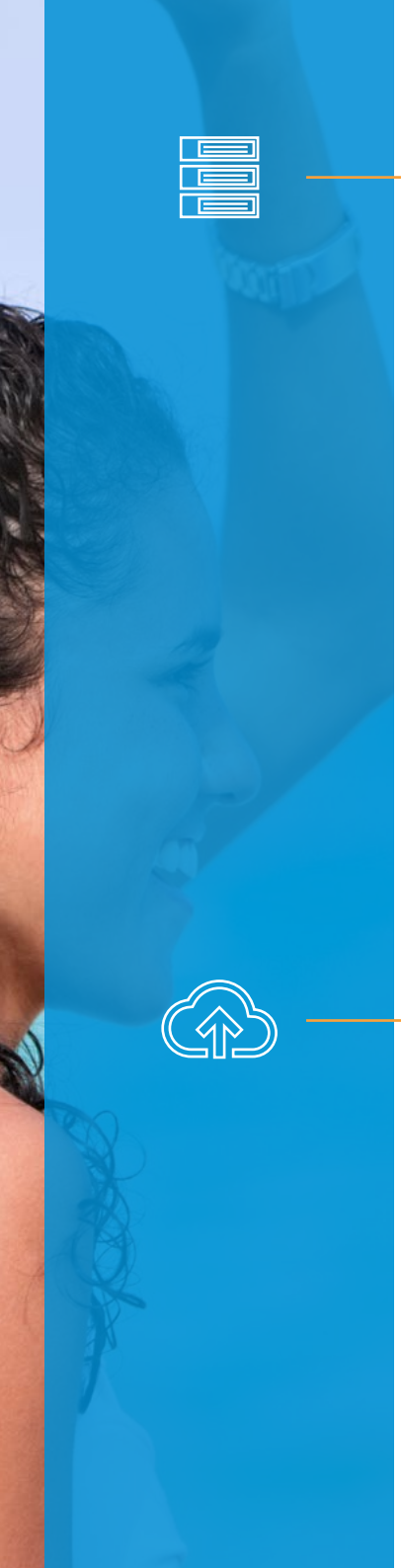
Vertrauen ist gut, Kontrolle ist besser

Automatisieren Sie Ihre Backup-Tests, so sparen Sie Zeit und stellen sicher, dass Ihre Backups auch während Ihrer Urlaubsabwesenheiten weiter laufen.

Nur wenige Backup-Hersteller bieten automatisierte Backup "Wiederherstellungstests" an. ActiveImage Protector bietet diese Möglichkeit seit Juni 2017 und sendet auch Fehlerbenachrichtigungen. Die zuletzt erstellte Backup-Datei wird automatisch als virtuelle Maschine in Hyper-V gestartet. Unterstützung von VMware und VirtualBox folgt in Kürze. Die so erstellte Maschine wird automatisch entfernt und es entstehen keine Engpässe bei der Speicherkapazität.

Behalten Sie die Kontrolle über Off-Site-Backup-Kopien

Dies ist ein wiederkehrendes Thema in den letzten Jahren: Die Erpressersoftware verschlüsselt alle Dateien auf Ihrem Netzwerk. CryptoLocker und WannaCry Angriffe hatten Millionen von Opfern. Ist Ihr Backup einmal verschlüsselt, wird eine Wiederherstellung unmöglich. Deshalb ist es wichtig, die zuvor erwähnte 3-2-1 Backup-Strategie zu implementieren.



Kontrolle des Zeitplans der Off-Site Speichermedien

Bandlaufwerke oder entfernbare USB-Laufwerke werden häufig für die Speichermedienrotation in IT-Umgebungen kleinerer und mittlerer Unternehmen eingesetzt. In Urlaubszeiten kann sich dieser Prozess jedoch als unzuverlässig erweisen.

Die meisten Backup-Anwendungen werfen das Medium von Wechseldatenträger-Technologien wie z.B. Tandberg Data RDX QuikStor automatisch aus, sobald das Backup abgeschlossen ist. Auf diese Weise hat die verantwortliche Person eine sichtbare Kontrolle über den Status der Sicherung. Darüber hinaus erhält er eine Erinnerung das Medium zu entfernen und Off-Site zu lagern.

Overland Tandberg bietet eine alternative Lösung mit RDX QuikStation, einem Wechseldatenträger- System mit 4 oder 8 RDX Laufwerken. Die QuikStation bietet verschiedene Betriebsarten. Die Wahl des Festplatten-Autoloader-Modus ermöglicht die Durchführung eines automatisierten Wechsels durch alle Steckplätze, optional ohne manuelle Intervention. Dies ist besonders während der Urlaubszeit hilfreich, wenn keine Vertretung verfügbar ist.

Sorgen Sie für konsistente und wiederherstellbare Cloud hosted Backups

Wenn Sie Ihre Backup-Dateien in der privaten Cloud speichern, vergessen Sie nicht die Installation von NetJapans kostenfreien Imagecenter LE am Remote Standort sowie die Aktivierung der automatisierten Backup-Testfunktion. Alternativ können Sie regelmäßige Live-Tests von Off-Site-Backup-Ketten dem kostenfreien ImageBoot-Installer durchführen. Sie benötigen nur 2 Minuten um die Kette in einer VM zu booten!

Bei Verwendung der öffentlichen Cloud wird die Überprüfung der Off-Site Backup-Dateien schon komplizierter. Daher ist es wichtig, dass Sie die Wiederherstellbarkeit Ihrer Backup-Dateien testen, bevor diese repliziert werden.

Remote-Zugriff sicherstellen für den Notfall-Failover!

Verwenden Sie ActiveImage Protector in Verbindung mit QuikStor oder QuikStation, so wählen Sie einfach zwischen den verschiedenen Optionen der Wiederherstellung Ihrer Backup-Dateien oder dem Zeitpunkt der Wiederherstellung, abhängig von der Art der Katastrophe oder der Wiederherstellungszeit.

Einrichten eines Notfall-Failover

ImageBoot ist eine Failover-Lösung, die im ActiveImage Protector enthalten ist. ImageBoot bootet eine virtuelle Notfallmaschine in Hyper-V, VMware oder VirtualBox mit der ausgewählten Backup-Datei.

Bevor Sie auf Urlaub gehen, stellen Sie sicher, dass ImageBoot auf mehreren Maschinen Ihres Netzwerks installiert ist und nicht nur auf Ihrem geschäftskritischen Server (für den Fall eines Serverabsturzes oder Cyber-Angriffs) und prüfen Sie die Remoteverbindung. Nach Start des Images werden Backups weiterhin auf demselben Speichermedium erstellt, vorausgesetzt Sie konfigurieren die Backups (im Failover-Modus) so, dass sie immer am selben Ort erstellt werden. Prüfen Sie die Einstellungen, bevor Sie auf Urlaub gehen, es kostet Sie nur 2 Minuten Ihrer Zeit!

Beachten Sie, dass Failover Szenarien nur für den Notfall gedacht sind und diese Maschinen nur für einen begrenzten Zeitraum laufen sollen, auch wenn es sich dabei um sehr leistungsfähige Maschinen handelt. Eine Wiederherstellung wird irgendwann notwendig. Allerdings hilft ein solches Failover-Verfahren Ihrem Unternehmen die Geschäftstätigkeit in nur 5-15 Minuten wieder aufzunehmen. Sie setzen Ihren Urlaub ungestört fort und führen nach Ihrer Rückkehr die Wiederherstellung mit Tandberg RDX Laufwerken aus.

Wiederherstellung nach Ihrem Urlaub

Die Wiederherstellung kann warten bis Sie aus Ihrem Urlaub zurück sind, umso besser. Andernfalls stellen Sie eine Remote-Verbindung zu ActiveImage Protector Recovery-Umgebung her und verwenden den Recovery-Assistenten um die ausgefallene Maschine wiederherzustellen. In der Zwischenzeit arbeiten die Mitarbeiter auf der virtuellen Failover-Maschine.

Bei einem Hardware-Ausfall organisieren Sie sofort das Ersatzgerät, sodass es nach Ihrer Rückkehr aus dem Urlaub bereits einsatzbereit ist. (Organisieren neuer Hardware/Server würde die Wiederherstellungszeit erhöhen, wenn Sie keine schnelle Failover Lösung wie ImageBoot haben).

Die Bedeutung des Failbacks

Failback ist der Vorgang der Wiederherstellung Ihrer Failover-Lösung zu einem permanenten Zustand oder physischer Hardware. Dazu ist es wichtig, dass Ihre Failover-Lösung weiterhin Backups zu einem zugänglichen Speicherplatz erstellt.

Wir empfehlen Ihnen ein Backup zu erstellen, bevor Sie die Failover-VM herunterfahren und diese über den Recovery–Prozess mit ActiveImage Protector auf dem neuen Server wiederherstellen. Auf diese Weise sind Sie sicher, dass alle Änderungen auf dem virtuellen Notfall-Server gespeichert und auch langfristig abrufbar sind.

Fazit

Die Urlaubszeit ist oft stressig für IT-Fachleute und die steigende Zahl an Cyber-Attacken erhöht den Druck, Schutzmaßnahmen allein genügen nicht. Ein verlässliches Backup, das Sie im Notfall den ursprünglichen Zustand Ihres Servers einfach und schnell wiederherstellen lässt, ist unabdingbar.

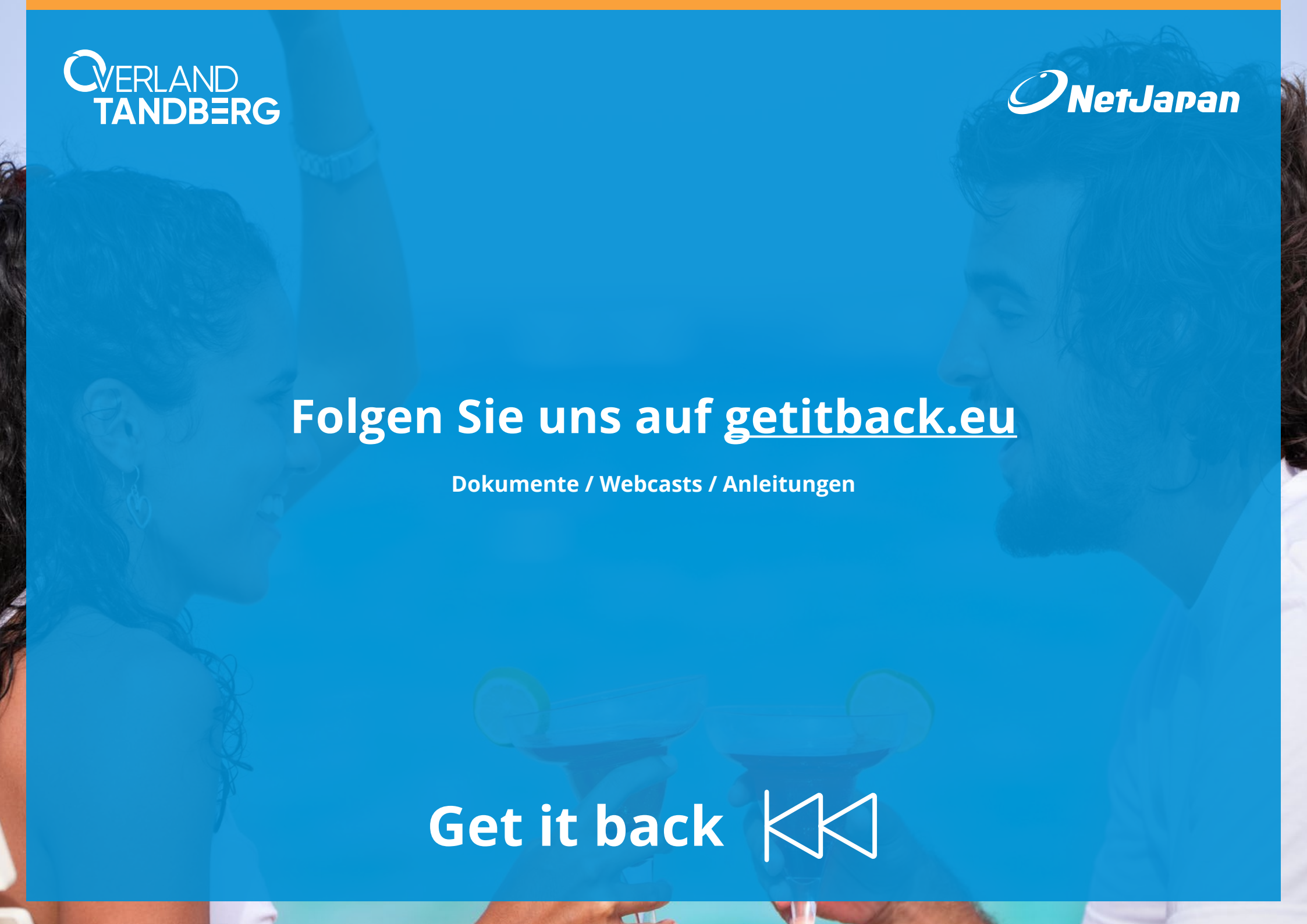
Vertrauen in Ihre Backup-Lösung ist gut, aber Kontrolle der Situation ist besser.

Kleine und mittlere Unternehmen erreichen einen hohen Grad an Schutz für Ihre Backup-Dateien durch die Kombination von **Tandberg RDX QuikStor** oder **QuikStation mit NetJapan ActiveImage Protector** Backup & Disaster Recovery Lösungen; so nehmen Unternehmen schnell wieder die Geschäftstätigkeit nach einem Katastrophenfall auf.

Erfahren Sie mehr zur optimalen Kombination und Konfiguration der beiden Lösungen und lesen Sie unsere Anleitungen:

Konfigurieren von QuikStor mit ActiveImage Protector

Konfigurieren von QuikStation mit ActiveImage Protector (in Kürze verfügbar)


OVERLAND TANDBERG
NetJapan
Folgen Sie uns auf getitback.eu
Dokumente / Webcasts / Anleitungen
Get it back