Sparen Sie Zeit
Artikel 32 –EU DSGVO: Sicherheit der Verarbeitung

Die EU-Datenschutz-Grundverordnung 2016/679 (DSGVO) trat am 25. Mai 2018 in Kraft. Kapitel IV - Kontrolle und Verarbeitung, Abschnitt 2: Sicherheit personenbezogener Daten, Artikel 32: “Sicherheit der Verarbeitung “ richtet sich insbesondere an Wiederverkäufer und IT-Dienstleister.

In diesem Leitfaden werden wir analysieren, welche Auswirkungen sich für Wiederverkäufer und Subunternehmer ergeben und wie sichergestellt werden kann, dass alle neuen Maßnahmen einfach implementiert und überwacht werden.

Das gesamte Kapitel IV der DSGVO ist hier nachzulesen.

NetJapan

Was besagt Artikel 32 der DSGVO?

1. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete **technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:
    a. die Pseudonymisierung und **Verschlüsselung** personenbezogener Daten;
    b. die Fähigkeit, **die Vertraulichkeit**, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
    c. die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen **bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen**;
    d. ein Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung** der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

2. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder **unrechtmäßig, oder unbefugte Offenlegung** von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
3. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
4. Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Notwendige Maßnahmen zur Anwendung des Artikels der DSGVO

Wiederverkäufer und IT-Dienstleister sind verantwortlich für die Beratung von Unternehmen, die Aufzeichnungen über Kunden und / oder Mitarbeiter führen (dies ist in 99% der Unternehmen der Fall) um die von der DSGVO geforderten Maßnahmen umzusetzen. Die Backups müssen:

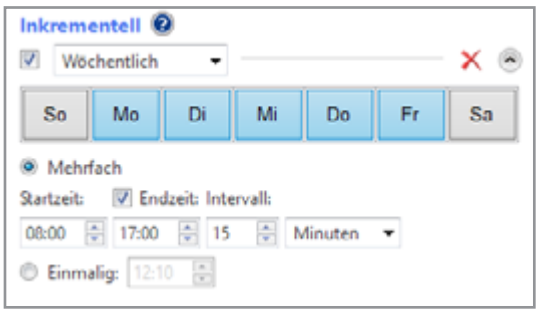
1. **automatisiert und regelmäßig erfolgen** um das Risiko von Datenverlust zu verringern (Punkt 2).
2. **verschlüsselt** sein (Punkt 1.a)
3. **passwortgeschützt sein,** um die Vertraulichkeit von Informationen zu wahren (Punkt 1.b.)
4. **Eine Kopie muss außerhalb des Firmennetzwerks** an einem anderen Ort gespeichert sein (Punkt 1.c.).
5. **Nur zugänglich für berechtigte Personen** (Punkt 1.b, Punkt 2 und Punkt 4)
6. **Getestet** (Punkt 1.d.)
7. **Regelmäßig überwacht** (Punkt 1.d)
8. **Jederzeit** innerhalb einer bestimmten Zeit **wiederhergestellt werden können**

Wie setzt man den Artikel 32 der DSGVO in der Praxis um?

Planen Sie automatisierte regelmäßige Backups

Je kürzer der Zeitintervall zwischen den einzelnen Backups ist, desto geringer das Risiko des Datenverlustes und desto höher ist der Schutz des Unternehmens!

NetJapan empfiehlt alle 5 Minuten eine inkrementelle Sicherung. Diese inkrementellen Sicherungen sind in ActiveImage Protector sehr klein, da nur geänderte Sektoren gespeichert werden. Die Realität zeigt jedoch, dass IT-Fachhändler und IT-Dienstleister nur 1x pro Stunde oder sogar nur 1x pro Tag eine inkrementelle Sicherung einrichten. Wir empfehlen Ihnen in jedem Fall mindestens 3 inkrementelle Sicherungen pro Tag einzuplanen!

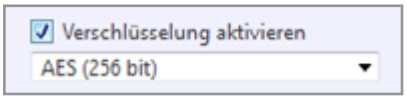


ActiveImage Protector Lösungen unterstützen Windows und Linux Systeme in physischen und virtuellen Umgebungen.

	PRODUKTNAME		AGENT-/ HOST-BASIEREND	BETRIEBS-SYSTEM
FÜR VIRTUELLE UMGEBUNGEN	ActiveImage PROTECTOR	ActiveImage Protector **Hyper-V Enterprise**	Host-basierend	
		ActiveImage Protector **Virtual – Unlimited**	Agent auf jeder VM	
		ActiveImage Protector **Virtual – Cloud**		
		ActiveImage Protector **Virtual – Single**	Agent-basierend	
		ActiveImage Protector **Virtual – 3 VM Pack**		
FÜR PHYSISCHE & VIRTUELLE		ActiveImage Protector **Server**	Agent-basierend	
		ActiveImage Protector **SBS**		
		ActiveImage Protector **Desktop**		
FÜR CLUSTER		ActiveImage Protector **Cluster**		
ADD-ON	ActiveVisor	**ActiveVisor**	Agent-basierend	
	ImageBoot	**ImageBoot**		
	ImageCenter LE	**ImageCenter** LE		
	vStandby AIP	vStandby **AIP**		

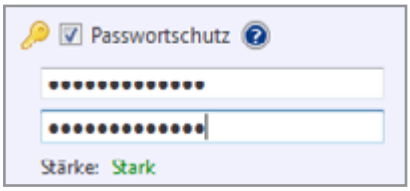
Verschlüsseln der Backups

Backups können in allen ActiveImage Protector Lösungen mit AES-256 verschlüsselt werden.



Schützen Sie Ihre Backups mit einem Passwort

Geben Sie bei der Backup-Erstellung ein Passwort ein, um den Zugriffsschutz zu aktivieren. Bewahren Sie dieses Passwort sicher auf, Sie benötigen es wieder bei der Wiederherstellung.



Speichern Sie eine Kopie der Backups außerhalb Ihres Büros /Netzwerks

Warum sollten Sie eine Kopie der Backups außerhalb Ihres Netzwerks aufbewahren?

Zum Schutz vor Malware-Angriffen!

Ransomware wird heutzutage auch über das Netzwerk verbreitet und Sie möchten nicht, dass Ihre Backups von Angreifern verschlüsselt werden, wenn eine Wiederherstellung notwendig ist.

Warum sollten Sie eine Kopie der Backups außerhalb der Räumlichkeiten Ihres Unternehmens aufbewahren?

Auch wenn die Wahrscheinlichkeit, dass Ihr Speichergerät gestohlen oder Opfer einer Naturkatastrophe wird, relativ gering ist, verlangt das EU-Datenschutzgesetz, dass Unternehmen auf solche Ereignisse vorbereitet sind.

Wie erstellt man eine Kopie des Backups außerhalb des Unternehmensnetzwerks und der Räumlichkeiten des Unternehmens?

Je nach Kundeninfrastruktur, Internetverbindung, Vertraulichkeit der gespeicherten Daten und jeweiligen Bedürfnisse, können wir folgendes empfehlen:

Backup Strategie - Medienrotation

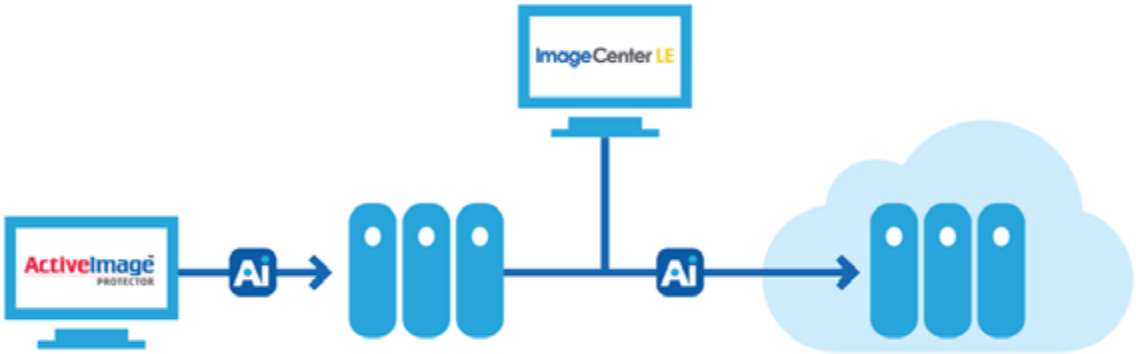
Verwenden Sie ActiveImage Protector und ImageCenter (kostenfrei) in Kombination mit Overland-Tandbergs RDX Lösungen als effektive und sichere Strategie. Wählen Sie:

- **ActiveImage Protector und ImageCenter mit QuikStor**
  Ein RDX Medium wird als Speicherplatz im Netzwerk verwendet während ein zweites RDX Medium an einem sicheren Ort aufbewahrt wird, zum Beispiel im Haus des IT-Managers oder des Geschäftsführers /Eigentümers des Unternehmens. Wählen Sie einen Tresor von Qualität, der Explosionen und Feuer stand hält.

- **ActiveImage Protector und ImageCenter mit QuikStation**
  Die QuikStation bietet extra Flexibilität mit einer möglichen Rotation bis zu 8 RDX Medien.

Backup Strategie mit Off-Site Backup

Speichern Sie eine Kopie Ihrer Backup-Datei in einer anderen Zweigstelle Ihres Unternehmens, beim Fachhändler/IT-Dienstleister oder in der Cloud.



Backup Zugriff begrenzen

Das Gesetz ist klar: Daten und Backups dürfen nur von autorisierten Personen abgerufen werden, sei es innerhalb des Unternehmens oder auch an jedem Ort außerhalb.

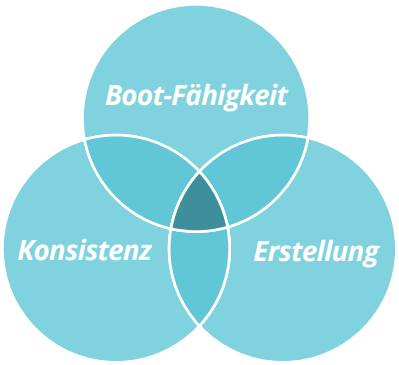
- Sie bewahren Backups in einer Zweigstelle auf: Stellen Sie sicher, dass sich die Backups nicht im selben Netzwerk befinden.
- Sie bewahren Ihre Backups im Unternehmen des IT-Fachhändlers auf: Stellen Sie sicher, dass Sie ein Dokument über den Aufbewahrungsort dieser Daten signieren und gleichzeitig muss gewährleistet sein, dass alle Personen mit physischen Zugriff auf den Backup-Dateiraum ebenfalls ein Vertraulichkeits- und Haftungsdokument unterzeichnen.
- Sie replizieren Ihre Backups in die Cloud: Kunden müssen über den Sicherheitsstandard und Ort des Datencenters informiert werden, wo die Backups aufbewahrt werden.

NetJapan bietet Cloud-Speicher. Das Rechenzentrum ist Tier III und befindet sich in der Schweiz. Dieses Datencenter wendet die Sicherheitsregeln des Europäischen Datenschutzgesetzes mit biometrischem Zugang und geschützten Räumlichkeiten vor möglichen Überschwemmungen, Bränden und anderen Sicherheitsbedrohungen, an.

Automatisches Testen der Backups

Es ist wichtig anzumerken, dass es unterschiedliche Arten der Verifizierung gibt. Die verschiedenen Backup-Lösungen auf dem Markt erlauben es Ihnen nicht, die gleichen Dinge zu überprüfen und dies könnte eventuell zu Ihrem Problem werden.

- Überprüfen Sie die korrekte Erstellung der Backups: Sie könnten durch ein technisches Problem der Software, ein unerwarteter Fehler des VSS-Dienstes oder durch keinen freien Speicherplatz (insbesondere bei fehlender Aufbewahrungsrichtlinie) verhindert werden.
- Überprüfen Sie die Konsistenz der Backups: Wenn die inkrementelle Kette durch eine einzelne beschädigte Datei korrumpiert ist, können Sie von diesem Zeitpunkt aus nichts mehr wiederherstellen und alle weiteren Daten gehen verloren.
- Überprüfen Sie die Boot-Fähigkeit der Backups: Eine korrekte Ausführung der Backups und eine konsistente Backup-Kette sind keine Garantie dafür, dass Sie die Backups wiederherstellen und starten können!

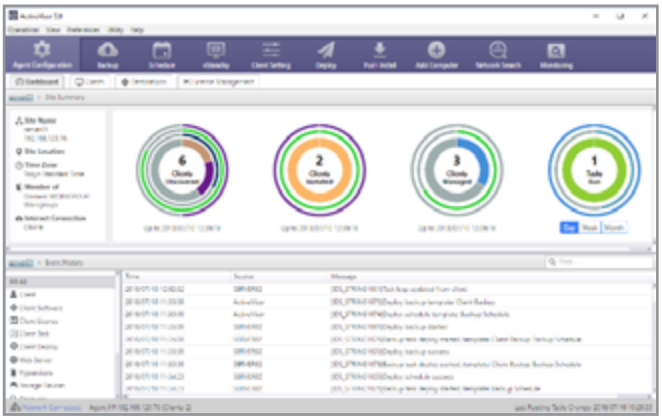


Weitere Informationen zu NetJapans Möglichkeiten der Backup-Überprüfung und Backup-Tests finden Sie in unserer Dokumentation Sparen Sie Zeit: Automatisieren Sie den Test Ihrer Backup-Dateien!

Fortlaufende Überwachung

Die manuelle Überwachung einer kompletten Backup-und Replikationsaufgabe kann Probleme bereiten. Verwenden Sie ein automatisiertes Überwachungstool oder noch besser, eine unabhängige Remote Management und Monitoring Plattform (RMM).

ActiveVisor



ActiveVisor wurde von NetJapan entwickelt zur Überwachung der ActiveImage Protector Aktivitäten:

- Backup Aufgaben Status
- ActiveImage Protector Dienste
- vStandby Dienste
- Lizenzstatus
- Remote Installation der ActiveImage Protector Agenten auf jedem beliebigen Netzwerk via VPN
- Verteilung vorkonfigurierter Backup/vStandby-Aufgaben/Zeitpläne
- System-Gruppierung

ActiveVisor ist nun auf Englisch verfügbar. Weitere Informationen zu ActiveVisor.

Hinweis: ActiveVisor meldet derzeit noch keine ImageCenter Aktivitäten (Replikation, Konsolidierung, Verifizierung, Boot-Test). Wenn Sie diese Aktivitäten überwachen möchten oder mehrere Endanwender ohne VPN gleichzeitig verwalten möchten, lesen Sie bitte weiter in diesem Dokument, da wir die Lösung für Sie bereit haben.

Überwachen Sie die gesamte IT Ihrer Kunden mit Server-Eye

Server-Eye ist ein deutsches Remote Monitoring und Management Tool. Es ist sehr intuitiv und zu einem attraktiven Preis erhältlich. Das RMM Tool überwacht Log-Dateien, die von unterschiedlichen IT-Lösungen erstellt werden (Verwaltet Backups, Patches, Supporttickets, Antivirenprogramme usw.), remote und sammelt die Informationen in einer Webkonsole, um Sie auf mögliche Probleme oder Risiken aufmerksam zu machen. Durch die Konsolidierung aller Informationen können Sie die richtigen Entscheidungen und Maßnahmen treffen.

servereye Managed Solution Partner

Durch die komplette Integration, liefert Server-Eye mehr Informationen zu NetJapan als zu jedem anderen Backup-Anbieter.

Im Folgenden finden Sie eine Liste der Funktionen, die Sie einfach anhand Ihrer Backup-Strategie in der Server-Eye Webkonsole überwachen und verwalten können:

- **ActiveImage Protector**
  - Backup Aufgabenstatus
  - ActiveImage Protector Dienst
  - Lizenzstatus (Version)

- **ImageCenter LE**
  - ImageCenter LE Dienst
  - Replikation
  - Konsolidierung
  - Backup Verifizierung
  - Boot-Check (Backup Boot-Fähigkeitsprüfung)
- **vStandby AIP**
  - vStandby Dienst
  - Konvertierungsaufgabe: Bereitschaftssysteme, die im Katastrophenfall sofort gestartet werden können.
- **Folgende Funktion sind mit Server-Eye auch im Webbrowser verfügbar:**
  - Push-Installation ActiveImage Protector Agenten aus einem abweichenden Netzwerk
  - Verteilen Sie eine vorkonfigurierte Backup-Aufgabe (weitere Informationen unten)
  - Richten Sie für den Fehlerfall Warnmeldungen per E-Mail oder SMS auf Ihr Smartphone ein.

Mehr zu NetJapan – Server-Eye Integration

Schritt für Schritt Anleitung: Einrichtung der Server-Eye Sensoren für NetJapan

Wiederherstellung in einem angemessenem Zeitrahmen

Artikel 32 der DSGVO geht über das frühere Datenschutzrecht hinaus und verlangt, dass innerhalb einer angemessenen Zeit wiederhergestellt werden kann.

Es ist wichtig die verschiedenen Arten der Wiederherstellung zu vergleichen, abhängig von der Art der Katastrophe, ob sie vor Ort oder extern stattfindet und wie lange es dauert bis das letzte nutzbare Backup betriebsbereit ist. KMU haben notwendigerweise nicht die gleichen Bedürfnisse wie große Unternehmen... das bedeutet jedoch nicht, dass sie Zugeständnisse bei der Wiederherstellungszeit machen müssen!

Verschiedene Arten der Wiederherstellungsstrategie für alle Unternehmen: Klein, Mittel, Groß und in weniger als 5 Minuten:

1. **Dateien/Ordner wiederherstellen durch öffnen der Backup-Dateien**
   Öffnen Sie eine ausgewählte Backup-Datei als Laufwerk, um eine oder mehrere Dateien abzurufen. Einfach und schnell!

2. **Wiederherstellen von Dateien/Ordnern mit ImageExplorer**
   Beinhaltet den Zugriff auf Dateien mit nur einem Mausklick und ohne Risiko für Benutzer die Backup-Kette abzuändern, da hierbei immer ein Lesezugriff ohne Schreibzugriff erfolgt.

3. **Komplettes System in nur 2 Minuten verfügbar– für temporäre Notfall-Nutzung**
   Starten Sie ein Backup als virtuelle Maschine in VMware (Workstation oder Player), Microsoft Hyper-V oder Oracle VirtualBox in nur 2 Minuten.
   ImageBoot macht es möglich! Verwenden Sie die erstellte virtuelle Maschine als funktionsfähigen temporären Ersatz. Alle Änderungen der Benutzer dieser virtuellen Maschine werden in einer differentiellen Datei gespeichert, ohne dass die ursprüngliche Backup-Kette geändert wird.

4. **Komplettes System in 2 Minuten verfügbar – für dauerhaften Einsatz**
   Dies ist möglich, indem eine virtuelle Replika Maschine eines physischen oder virtuellen Produktivsystems erstellt wird, die automatisch aktualisiert wird und im Notfall sofort auf einem regulären Hypervisor gestartet werden kann.
   Diese Funktion von vStandby und vStandby AIP ist ein Angebot von NetJapan, erstere ist in ActiveImage Protector enthalten und zweitere ist ein zusätzliches Modul, das auf jeder beliebigen Maschine des geschützten Netzwerks installiert werden kann, auch Off-Site!
5. **Wiederherstellung virtueller Maschinen**
   Einige Lösungen wie ActiveImage Protector Hyper-V ermöglichen Ihnen die Verwendung einer virtuellen Maschine, während die Wiederherstellung im Hintergrund läuft. Sehr praktisch in einer Microsoft Hyper-V Umgebung, damit die Benutzer so schnell wie möglich wieder arbeiten können.

Zu beachten ist, dass das Sichern von einzelnen Daten in einem kompletten Desaster-Fall eine sehr lange Wiederherstellungs- und Bereitstellungszeit erzeugt.

Es ist auch wichtig anzumerken, dass im Falle einer Image-Backup-Strategie oft eine Bare-Metal-Wiederherstellung enthalten ist (Architecture Independent Restore-Funktion - oder kurz AIR - in ActiveImage Protector). Dies kann jedoch auch sehr lange dauern. Daher ist es erforderlich, dass Unternehmen schnellere Wiederherstellungslösungen wie die oben genannten zur Kenntnis nehmen und implementieren.

Backup und Disaster Recovery Strategie Szenarien entsprechend Artikel 32 der DSGVO

Szenario 1 - Für KMU, oder Unternehmen, die sehr vertrauliche Daten speichern oder nur über eine begrenzte Internetverbindung verfügen

Infrastrukturtyp (Beispiel)

- 1 Server Windows und/oder eine oder mehrere VMs
- 1 NAS

Backup Strategie

- Installieren Sie ActiveImage Protector auf den Systemen, die gesichert werden sollen
- Installieren Sie ImageCenter auf einem System im Netzwerk
- Erwerben Sie ein RDX-Gerät mit mindestens 2 Medien (eines davon wird verwendet während das zweite an einem sicheren Ort aufbewahrt wird)

1. Konfigurieren Sie eine automatisierte Backup-Aufgabe in ActiveImage Protector, mit einem Voll-Backup pro Woche und einem inkrementellen Backup zu jeder Stunde während der Geschäftszeiten, mit einem NAS als Ziel.
2. Legen Sie in ActiveImage Protector die Aufbewahrungsrichtlinie in Abhängigkeit vom verfügbaren Speicherplatz auf dem NAS fest. In diesem Beispiel behalten wir immer die letzten 3 Wochen.

3. Konfigurieren Sie das ImageCenter, um eine Kopie der Sicherungsdateien auf das RDX-Gerät zu replizieren und täglich die RDX-Medien zu rotieren.
   Lesen Sie unsere RDX Konfigurationsanleitung

Erhöhen Sie die Sicherheit

1. Automatisierte Verifizierung und Backup-Tests
   a. Verwenden Sie ImageCenter zur Prüfung der Backup-Konsistenz.
   b. Option: Installieren und verwenden Sie Microsoft Hyper-V zusammen mit der ImageCenter BootCheck Funktion und testen Sie automatisiert die Boot-Fähigkeit - Anleitung.
   c. Parallel dazu verwenden Sie ImageBoot ein- oder zweimal pro Jahr, um eine ausgewählte Sicherungsdatei in nur zwei Minuten auf einer VM zu starten. Mit diesem Verfahren können Sie auf das gesamte System, alle Anwendungen und Daten zugreifen, um zu überprüfen, ob im Katastrophenfall alles funktioniert.
2. Monitoring
   a. Option 1: Implementieren Sie E-Mail-Warnungen in ActiveImage Protector und ImageCenter im Falle eines Fehlers
   b. Option 2: Überwachen Sie mit ActiveVisor
   c. Option 3: Überwachen Sie die ActiveImage Protector und ImageCenter Aktivitäten in Ihrem Navigator mit Server-Eye - Anleitung.
3. Bewahren Sie ein RDX Medium an einem sicheren Ort auf, außerhalb Ihres Unternehmens während das zweite RDX Medium im Einsatz ist.

Strategie zur Wiederherstellung

Verwenden Sie ImageBoot im Katastrophenfall. Diese Funktion kann vorab installiert werden, z. B. auf einem relativ leistungsstarken Windows 10 Pro-System mit aktiviertem Microsoft Hyper-V. Dieser Computer könnte auch vom IT-Fachhändler / IT-Dienstleister zur Verfügung gestellt werden, während das Hauptsystem im Falle einer Katastrophe repariert wird, obwohl es besser wäre, wenn es vor einem solchen Ereignis bereits vor Ort wäre, da dies die Ausfallzeit verkürzen würde.

Diese Lösung sichert die Kontinuität der Arbeit. Es gibt minimale Einbußen hinsichtlich der Geschwindigkeit / Latenz des Ersatzsystems, aber Sie haben vollen Zugriff auf Ihr ausgefallenes System.

Eine Bare-Metal-Wiederherstellung im Katastrophenfall, während Benutzer die mit ImageBoot erstellte Notfallmaschine verwenden.

Möglichkeit zum Wiederherstellen von Dateien mit Image öffnen oder ImageExplorer-Funktion.

Szenario 2 – Für Unternehmen mit einer geeigneten Internet-Upload-Bandbreite

(Prüfen Sie, wie sich die Bandbreite auf die Backup-Übertragung auswirkt)

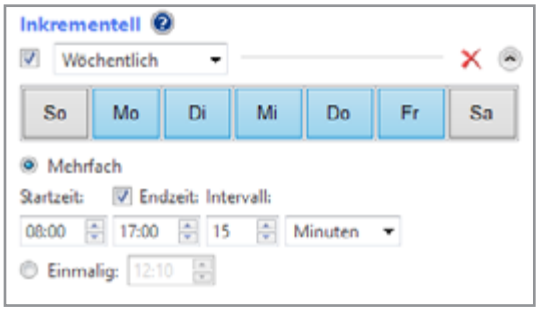
Infrastrukturtyp (Beispiel)

- 1 Server Windows und/oder eine oder mehrere VMs
- 1 NAS

Backup-Strategie

- Installieren Sie ActiveImage Protector auf den Systemen, die gesichert werden sollen
- Installieren Sie ImageCenter auf einem System im Netzwerk

- Installieren Sie ein Speichergerät und richten Sie einen FTP-Server am Remote-Standort außerhalb des Firmennetzwerks ein.
- Installieren Sie ImageCenter am Remote-Standort.



1. In ActiveImage Protector richten Sie ein einmaliges Voll-Backup und inkrementelle Backups zu jeder Stunde während der Geschäftszeiten, ein.
2. On-Site ImageCenter, einrichten:
   a. Konsolidierung und Aufbewahrung
   b. Automatisierte Backup-Konsistenz-Prüfung
   c. Automatisierter Backup Boot-Fähigkeitstest mit der BootCheck Funktion, falls Sie Microsoft Hyper-V installieren können (oder bereits verwenden).
   d. Replikation zum FTP Server. Wählen Sie zwischen dem Versand des Voll-Backups per Internet oder manuell per Kurier-Dienst.
3. Off-Site ImageCenter, einrichten:
   a. Automatisierte Backup-Konsistenz-Prüfung
   b. Automatisierter Backup Boot-Fähigkeitstest mit der Boot-Check Funktion, falls Sie Microsoft Hyper-V installieren können (oder bereits verwenden).
4. On-Site: Installieren Sie ImageBoot auf ein System im Netzwerk, um von Zeit zu Zeit manuelle Backup-tests durchzuführen.
5. Off-Site: Installieren Sie ImageBoot auf ein System im Netzwerk, um von Zeit zu Zeit manuelle Backup-tests durchzuführen. (Dies ist nicht notwendig wenn zuvor bereits Schritt 4 ausgeführt wurde. Es ist jedoch immer besser, alles erneut zu überprüfen. Wenn Sie also Schritt 5 implementieren können, tun Sie es.)

Erhöhen Sie die Sicherheit

6. Automatisierte Verifizierung und Backup-Tests
   a. Verwenden Sie ImageCenter zur Prüfung der Backup-Konsistenz.
   b. Option: Installieren und verwenden Sie Microsoft Hyper-V zusammen mit der ImageCenter BootCheck Funktion testen Sie automatisiert die Boot-Fähigkeit - Anleitung. Implementieren Sie dies On-Site und Off-Site.
   c. Parallel dazu verwenden Sie ImageBoot ein- oder zweimal pro Jahr, um eine ausgewählte Sicherungsdatei in nur zwei Minuten auf einer VM zu starten. Mit diesem Verfahren können Sie auf das gesamte System, alle Anwendungen und Daten zugreifen, um zu überprüfen, ob im Katastrophenfall alles funktioniert.
7. Monitoring: Installieren Sie Server-Eye Sensoren On-Site und Off-Site (1 Sensor pro installiertem ActiveImage Protector und ImageCenter) nach dieser Anleitung.

Strategie zur Wiederherstellung

Ähnlich wie in Szenario 1. Sie können ImageBoot auch außerhalb des Standorts installieren und es als Notfall / temporäres Failover vom Remote-Standort aus.

Szenario 3 – Erweiterte Version von Szenario 2 für produktive Microsoft Hyper-V Umgebungen

Unternehmen, die in einer Microsoft Hyper-V-Umgebung arbeiten, können die ActiveImage Protector Virtual Edition installieren und ihre Backup-Strategie und Backup-Prüfungen wie in Szenario 2 konfigurieren.

Strategie zur Wiederherstellung

Installieren Sie vStandby AIP auf einem On-Site- und / oder Off-Site-Computer, um eine virtuelle Standby Replika (VSR) zu erstellen, die jederzeit im Falle eines Ausfalls oder einer Katastrophe startfähig ist.

Sie können diese VSR manuell für schnelle und einfache Wiederherstellungstests verwenden und Sie können ImageBoot weiterhin verwenden, um Sicherungen mehrmals pro Jahr manuell zu testen.

Zögern Sie nicht, uns zu kontaktieren, um Sie bei der Definition der besten Backup- und Disaster Recovery-Lösung zu unterstützen, die an Ihre Infrastruktur und Ihr Budget angepasst ist.

Fazit

1. Wir empfehlen, dass Sie niemals eine unqualifizierte Person für Backups einsetzen. Die professionelle Implementierung und Überwachung ist ein wichtiger Teil des Backup- und Wiederherstellungskonzepts.

2. Nach dem DSGVO vom Mai 2018 wird dringend empfohlen, nicht nur die Backup-Strategie, sondern auch Backup-Recovery- und Backup-Testprozesse zu überprüfen. Dies ist sehr oft die Schwachstelle eines Unternehmens.

3. Nicht genug Zeit, Ressourcen oder Wissen, um all dies umzusetzen? Unsere Experten helfen Ihnen und konfigurieren sogar alles per Remote-Sitzung. Besuchen Sie die NetJapan-Service-Seite.