Cybersicherheit stärken: Backups als Schlüssel zur NIS 2-Konformität

Freitag, 23. August 2024

Marco Horstmann

Senior Systems Engineer

Verordnungen innerhalb der EU/Deutschland

- BSI-Grundschutz
- VAIT (Versicherungsaufsichtliche Anforderungen an die IT)
- BAIT (Banken Anforderungen an die IT)
- KRITIS
- NIS2 (Network and Information Systems Directive)
- DORA – (Digital Operational Resilience Act)

Problem: Es gibt zu viele Verordnungen und Richtlinien die sich zum Teil überlappen. Die Unternehmen haben zusätzlich noch eine Vielzahl von Verordnungen und Richtlinien in anderen Bereichen. Wie z.B das Lieferkettengesetz.

IT relevante Rechte in Deutschland

Wir haben ja noch mehr!

- Cybersicherheitsgesetze:
  - Diese Gesetze regeln die Sicherheit von Informationssystemen und den Schutz vor Cyberangriffen. Beispiele sind die NISRichtlinie (Network and Information Systems Directive) und nationale Gesetze zur Cybersicherheit.
- Internationales IT-Recht:
  - Aufgrund der globalen Natur der Informationstechnologie gibt es auch internationale Abkommen und Vereinbarungen, die das grenzüberschreitende IT-Recht regeln.
- Datenschutzrecht:
  - Das Datenschutzrecht regelt die Erhebung, Verarbeitung, Speicherung und den Schutz personenbezogener Daten. Hierzu gehört die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union sowie nationale Datenschutzgesetze, wie das Bundesdatenschutzgesetz (BDSG) in Deutschland.
- Urheberrecht und geistiges Eigentum:
  - Das Urheberrecht schützt die geistigen Eigentumsrechte an Software, Inhalten und digitalen Kreationen. Dies umfasst auch Patente, Marken und Handelsgeheimnisse. Dies ist besonders Spannend im Hinblick auf die Nutzung von KI.
- E-Commerce-Gesetze:
  - Diese Gesetze regeln den elektronischen Handel und die Rechte und Pflichten von Unternehmen und Verbrauchern bei OnlineTransaktionen.

NIS2 Richtlinie

Höherer Schutz für die kritische Infrastruktur

Die weltweite Bedrohung durch Cyberangriffe hat in den letzten Jahren extrem zugenommen. Einzelne Länder, Behörden und Institutionen haben mit unterschiedlichen Richtlinien reagiert.

Seit dem 3.Mai 2016 gibt es in Deutschland die KRITIS Verordnung, wo Betreiber Kritischer Infrastrukturen angewiesen werden ihre Dienste gegen Cyberangriffe zu schützen.

In der EU gab es Bestrebungen eine ähnliche Richtline zu definieren, die in ihren Grundzügen in der gesamten EU gilt.

Der europäische Gesetzgeber hat im Dezember 2022 die Network-and-Information-Security-Richtlinie 2.0 (Richtlinie (EU) 2022/2555, „NIS2-RL“) verabschiedet.

Die IT-Sicherheitsgesetzgebung in der EU soll „zum reibungslosen Funktionieren ihrer Wirtschaft und Gesellschaft“ beitragen

NIS2 Richtlinie und Ziele

Verbesserung der Resilienz kritischer Infrastrukturen, Förderung der Zusammenarbeit zwischen EU-Mitgliedstaaten

"Dieses Foto" von Unbekannter Autor ist lizenziert gemäß CC BY-SA

Die Roadmap der NIS2 Richtlinie

Da es sich bei der NIS2-RL um eine Richtlinie handelt, ist sie (im Unterschied zur Verordnung) nicht unmittelbar in den Mitgliedstaaten anwendbar, sondern bedarf zunächst einer Transformation in nationales Recht. Der deutsche Gesetzgeber ist daher gehalten, die nationalen IT-Sicherheitsgesetze (insbesondere das BSIG, BSI-Gesetz) anzupassen

NIS2 Richtlinie, betroffene Sektoren

Die NIS2-RL weitet den bisherigen Anwendungsbereich deutlich aus und erstreckt sich nun auf 18 Sektoren, sowohl im öffentlichen als auch im privaten Bereich.

Als europäische Richtlinie ist für die Anwendbarkeit der NIS2-RL ein gewisser Bezug zur EU erforderlich.

SEKTOREN MIT HOHER KRITIKALITÄT (ANHANG I DER NIS2-RL):	SONSTIGE KRITISCHE SEKTOREN (ANHANG II DER NIS2-RL):
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmarktinfrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschung
Digitale Infrastruktur	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	

NIS2 Richtlinie, ab welcher Größe?

Die NIS2-RL ist zunächst auf jede Einrichtung der in den Anhängen I und II der NIS2-RL genannten Sektoren anwendbar, die nach der Terminologie des Europarechts die Schwellenwerte für mittlere Unternehmen überschreitet. Das ist grundsätzlich dann der Fall, wenn die Einrichtung mindestens 50 Beschäftigte hat oder einen Jahresumsatz bzw. eine Jahresbilanzsumme von mehr als 10 Mio. EUR erzielt.

WESENTLICHE EINRICHTUNG	WICHTIGE EINRICHTUNG
Sektor in Anhang I + mind. 250 Beschäftigte oder über 50 Mio. EUR Jahresumsatz bzw. über 43 Mio. EUR Jahresbilanzsumme	**Sektoren in Anhang I u. II +** mind. 50 Beschäftigte oder über 10 Mio. EUR Jahresumsatz bzw. Jahresbilanzsumme (soweit nicht bereits wesentliche Einrichtungen)
bestimmte Sonderfälle, z.B. Zentralregierung, DNS-Diensteanbieter oder staatliche Einstufung als wesentliche Einrichtung	bestimmte größenunabhängige Sonderfälle, z.B. staatliche Einstufung als wichtige Einrichtung

NIS2 Richtlinie, Unterschied zu KRITIS

Durch die umfassendere Definition des Anwendungsbereichs obliegt die Festlegung relevanter Sektoren nicht mehr den Mitgliedstaaten, die Schwellenwerte der deutschen BSI-Kritisverordnung dürften daher bald Geschichte sein.

NIS1-RL/BSI-KRITISVERORDNUNG	NIS2-RL
Energie	Energie
Wasser	Trinkwasser, Abwasser
Ernährung	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Informationstechnik und Telekommunikation	Digitale Infrastruktur
Gesundheit	Gesundheitswesen
Finanz- und Versicherungswesen	Bankwesen, Finanzmarktinfrastrukturen
Transport/Verkehr	Verkehr, Weltraum (teilweise), Post- und Kurierdienste,
Entsorgung	Abfallbewirtschaftung
	Verwaltung von IKT-Diensten (B2B)
	Öffentliche Verwaltung
	Produktion, Herstellung und Handel mit chemischen Stoffen
	Verarbeitendes Gewerbe/Herstellung von Waren
	Anbieter digitaler Dienste
	Forschung

NIS2 Richtlinie

NIS2…eine Management Aufgabe

Mit der NIS2-RL machte der europäische Gesetzgeber deutlich, dass er die Gewährleistung von Cybersicherheit und die Prävention von IT-Sicherheitsvorfällen als Aufgabe des obersten Managements jedes Unternehmens begreift. Gemäß Art. 20 Abs. 1 NIS2-RL müssen die „Leitungsorgane“ die Einhaltung von Risikomanagementmaßnahmen (dazu unten IV.) überwachen und – noch bedeutender – können für Verstöße in diesem Bereich (persönlich) verantwortlich gemacht werden.

WESENTLICHE EINRICHTUNGEN	WICHTIGE EINRICHTUNGEN
Geldbuße bis zu: **10 Mio. EUR** oder **2 % des gesamten weltweiten Vorjahresumsatzes des Unternehmens, dem die Einrichtung angehört**	Geldbuße bis zu: **7 Mio. EUR** oder **1,4 % des gesamten weltweiten Vorjahresumsatzes des Unternehmens, dem die Einrichtung angehört**

NIS2 Richtlinie, Anforderungskatalog

- Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,
- Bewältigung von Sicherheitsvorfällen,
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall sowie Krisenmanagement,
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit,
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit,
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung

NIS2 Richtlinie

Was bedeutet das für unsere Kunden?

- Mehr Kunden unterliegen der KRITIS Einstufung
- Stärkerer Fokus durch höhere Strafen
- Mehr Abstimmung bei den IT-Komponenten (Veeam und SOPHOS)
- Ggf. ein Redesign der IT
- Einführung eines “Information Security Management System” (ISMS)
- Mehr Personal wird gebunden

"Dieses Foto" von Unbekannter Autor
ist lizenziert gemäß CC BY-NC

Sektoren und Branchen KRITIS

Es gibt 9 KRITIS Sektoren, die auf Bundesebene festgelegt wurden. In der Novellierung des BSIG im Jahr 2012 wurde die Liste durch den Sektor „Siedlungsabfallentsorgung“ ergänzt.

Rechtlich verbindlich ab einer Versorgung von mindestens 500.000 Bürgern

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

Quelle: https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/Sektoren-Branchen/sektoren-branchen_node.html

Wie können wir als Veeam helfen?

Datensicherungskonzept nach IT-Grundschutz (Kritis)

CON.3:Datensicherungskonzept

- Fehlende Datensicherung
- Fehlende Wiederherstellungstests
- Ungeeignete Aufbewahrung der Datenträger von Datensicherungen
- Fehlende oder unzureichende Dokumentation
- Missachtung gesetzlicher Vorschriften
- Unsichere Cloud-Anbieter für Online-Datensicherungen
- Ungenügende Speicherkapazitäten
- Unzureichendes Datensicherungskonzept

Fehlende Datensicherung

Veeam One Reports: Protected VMs

VEEAM

Protected VMs

Description

This report lists protected and unprotected VMware vSphere and Microsoft Hyper-V VMs including their last backup job status.
Note: VM replicas created by Veeam Backup & Replication jobs are not accounted in this report.

Report Parameters

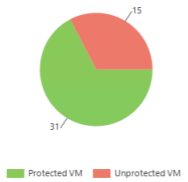
Scope:	Virtual Infrastructure
RPO:	24 hours (11/7/2021 12:00:00 PM)
VM exclusion rule:	
Job types:	VM Backup, Replication
Analyze VM templates:	No
Excluded jobs:	-

Summary

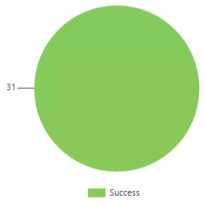
VMs Overview

Total VMs:	48
Including VM Replicas:	2
Protected VMs:	31
With Backup:	31
With Replication:	2
Unprotected VMs:	15

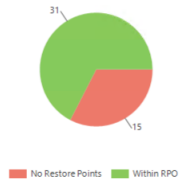
Protected VMs



VM Last Backup State



VM Last Backup Age



Report created: 11/8/2021 11:13:40 AM ((UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague)

Page: 1 of 4

Unprotected VMs (VMware)

Location: vc1.democenter.int>esx16.democenter.int

VM Name	VM Creation Date	Creator	VM Size (GB)	Available Restore Points	Last Backup (Replica) Date
Unprotected Time: No Backup					
demo-sql1	10/20/2021	DEMOCENTER\svc-demovao	16	-	-

Location: vc1.democenter.int>esx18.democenter.int

VM Name	VM Creation Date	Creator	VM Size (GB)	Available Restore Points	Last Backup (Replica) Date
Unprotected Time: No Backup					
drlab-hq-gw	11/3/2021	DEMOCENTER\svc-deployer	0	-	-

Location: vc1.democenter.int>hx-esx1.democenter.int

VM Name	VM Creation Date	Creator	VM Size (GB)	Available Restore Points	Last Backup (Replica) Date
Unprotected Time: No Backup					
demo-sql1 (1)	10/27/2021	DEMOCENTER\svc-demovao	165	-	-
stCtlVM-FCH2117V16G	Not defined	Not defined	121	-	-

Location: vc1.democenter.int>hx-esx2.democenter.int

VM Name	VM Creation Date	Creator	VM Size (GB)	Available Restore Points	Last Backup (Replica) Date
Unprotected Time: No Backup					
stCtlVM-FCH2117V10V	Not defined	Not defined	159	-	-

Location: vc1.democenter.int>hx-esx3.democenter.int

VM Name	VM Creation Date	Creator	VM Size (GB)	Available Restore Points	Last Backup (Replica) Date
Unprotected Time: No Backup					
stCtlVM-FCH2117V0PN	Not defined	Not defined	103	-	-

Location: vc1.democenter.int>hx-esx4.democenter.int

VM Name	VM Creation Date	Creator	VM Size (GB)	Available Restore Points	Last Backup (Replica) Date
Unprotected Time: No Backup					
stCtlVM-FCH2116V3WD	Not defined	Not defined	118	-	-

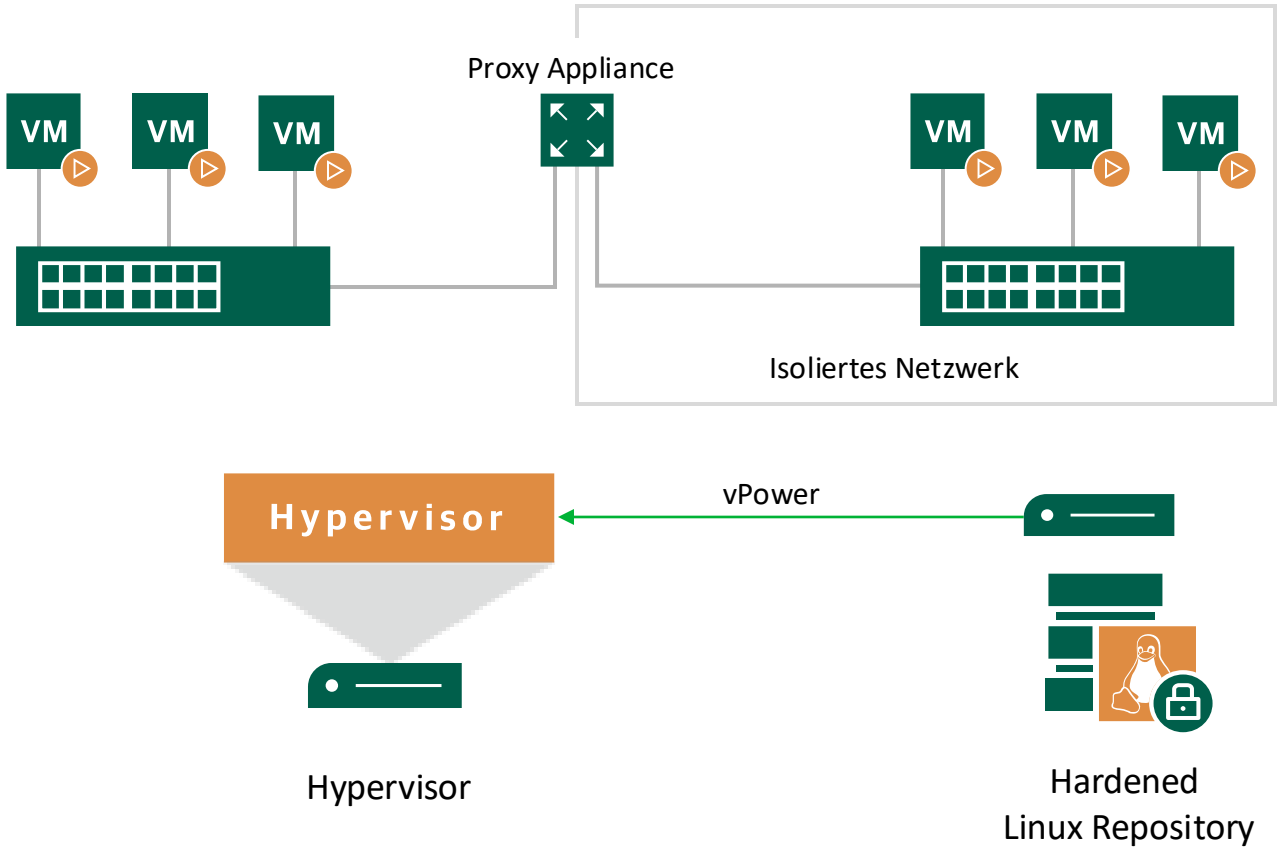
Location: vc1.demolab.local>dr-esx1.demolab.local

VM Name	VM Creation Date	Creator	VM Size (GB)	Available Restore Points	Last Backup (Replica) Date
Unprotected Time: No Backup					
mysql1_cdpreplica	4/13/2021	VSPHERE.LOCAL\svc-vbr	3	-	-
web1_cdpreplica	4/13/2021	VSPHERE.LOCAL\svc-vbr	3	-	-

veeam

Fehlende Wiederherstellungstests

vollständig automatisierte Wiederherstellungstests mit SureBackup™



SureBackup Job

- Ping
- Heartbeat
- Apps
- Report

Ungeeignete Aufbewahrung der Datenträger

Veeam bietet hier keine Abhängigkeiten

Herstellerunabhängige Backupablage (Repositorys)

- Windows Server
- Linux Server (Hardened)
- NAS Systeme
- LTO Bandlaufwerke
- Object Storage (Hardened)
- Deduplication Appliances (ggf. Hardened)

Eine mögliche Zusammenfassung durch ein Veeam SOBR

Empfohlenes Design nach der 3-2-1 Regel

Ungeeignete Aufbewahrung der Datenträger

Wiederherstellbarkeit - auch im Falle einer Ransomware Attacke

Verschiedene Kopien

Unterschiedliche Medien

Offsite Kopie

veeam

Air-gapped oder unveränderlich

Keine Fehler durch Restore-Tests

Fehlende oder unzureichende Dokumentation

Reports aus Veeam One und Dokumentation aus dem Veeam Disaster Recovery Orchestrator

VEEAM

Infrastructure Changes Audit

Description

This report tracks configuration changes in your virtual environment, providing detailed information about every change for each user.

Report Parameters

Scope:	Virtual Infrastructure
Reporting period:	1 week (2/12/2021 - 2/18/2021)
Object types:	Any Object Types
Users:	All
Sort by:	Time of Occurrence

Summary

Top 10 VMs with Changes

VM Name	Cluster/Host	# of Changes
apache07	esx02	15197
hpvsa01	esx01	762
proxy01	esx02	648
tech_srv01	esx02	497
dc03	esx02	240
dns01	esx02	240
apache02	esx01	108
backup01	esx02	88
tapesrv03	esx01	54
sandbox	esx01	30

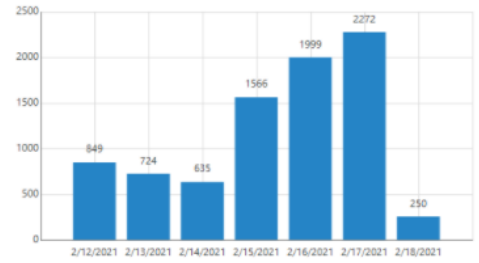
Top 10 Hosts with Changes

Host Name	# of Changes
esx02	2564
esx03	78
esx01	78

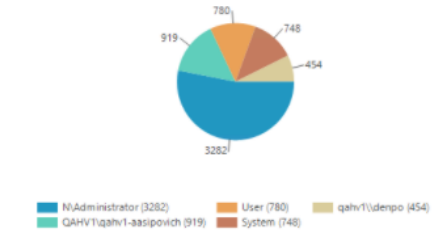
Top 10 Datastores with Changes

Datastore Name	# of Changes
esx02-ds1	3
datastore1	1

Number of Changes Made



Modifications per User (Top 5)



Test. Plan Group Details. 2/2/2018 2:41 AM

Plan Group Details

DR Test Group - Exchange Details

rl2016DC01

Back to DR Test Group - Exchange Summary

VM and Replica Details

Infrastructure	Source (Production)	Replica (DR)
VM Name	rl2016DC01	rl2016DC01_replica
Restore Point	N/A	Thursday, December 14, 2017 3:25 AM
Veeam Backup Server	U12R2VBR95	U12R2VBR95
vCenter	N/A	N/A
Cluster	N/A	N/A
Host	172.16.2.204	172.16.2.204
Datastore	Datastore2	Datastore2

Recovery result and duration

Result	Step Name	Start Time	Duration
✓ Success	Check VM license and availability	2:32:02 AM	00:00:00
✓ Success	Process Replica VM	2:32:02 AM	00:04:36
✓ Success	Check VM Heartbeat	2:36:38 AM	00:00:23

Recovery Step Details

Check VM license and availability

Timestamp	Details
2:32:02 AM	License has not expired
2:32:02 AM	License is not exceeded
2:32:02 AM	Waiting VM for availability...
2:32:02 AM	VM is ready for processing

Process Replica VM

Timestamp	Details
2:32:02 AM	Step 'Process Replica VM' execution started. Plan mode = StartTest
2:32:02 AM	1 execution attempt
2:32:52 AM	Starting VM...
2:33:05 AM	Powering on VM rl2016DC01_replica on host 172.16.2.204
2:33:35 AM	Waiting for VM to boot in 1092 sec
2:35:59 AM	VM was started successfully
2:36:38 AM	Step 'Process Replica VM' execution finished

veeam

Missachtung gesetzlicher Vorschriften

vollständig automatisierte Wiederherstellungstests mit SureBackup™

Gesetzliche Vorgaben wie:

- Die Aufbewahrungsfrist:
- GFS: Grandfather-Father-Son
- Backup Copy Job mit GFS
- Tape Job mit GFS
- Logic eines Veeam SOBR mit Copy and Move

Ein Ransomware Schutz:

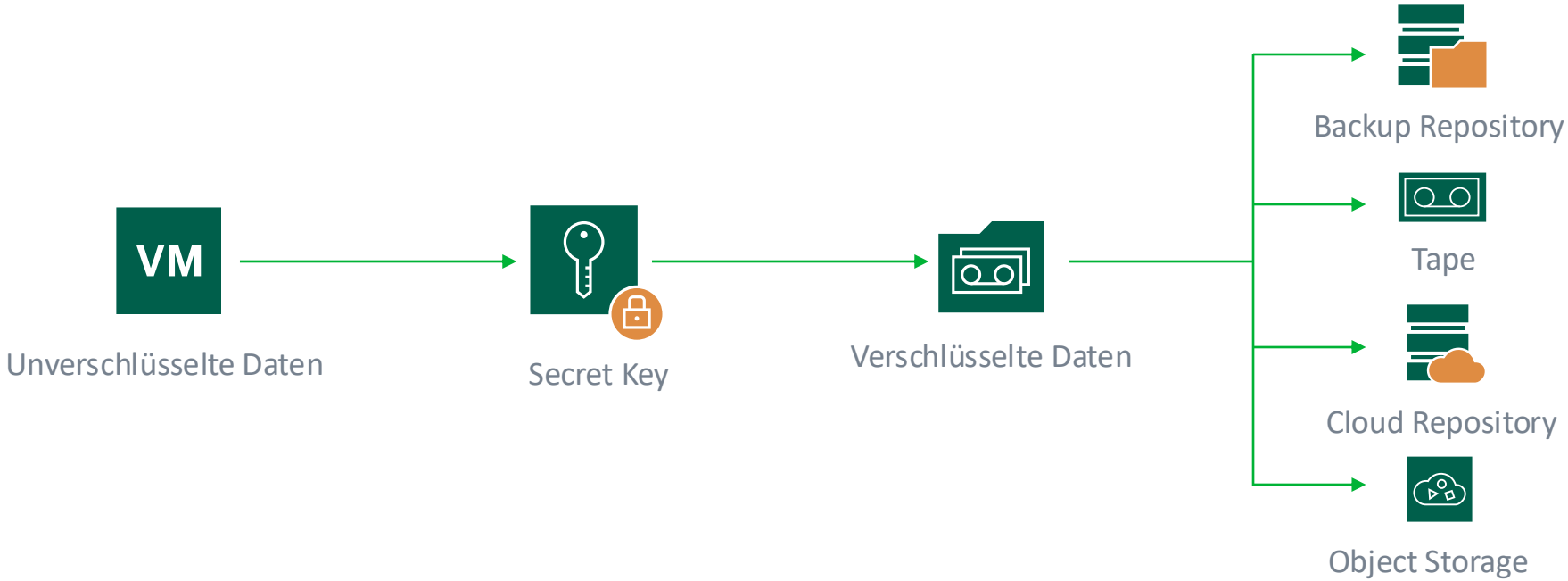
- Hardened Linux Repository
- Hardened Deduplication Appliance
- Immutability of Opject Storage

Unsichere Cloud-Anbieter für Online-Datensicherungen

vollständig automatisierte Wiederherstellungstests mit SureBackup™

Verschlüsselte Übertragung (in-flight)

Verschlüsseltes speichern (at-rest)



Ungenügende Speicherkapazitäten

VEEAM

Capacity Planning for Backup Repositories

Description

This report shows the dynamics of backup repository free space usage and identifies the date when the repository will run out of free space.

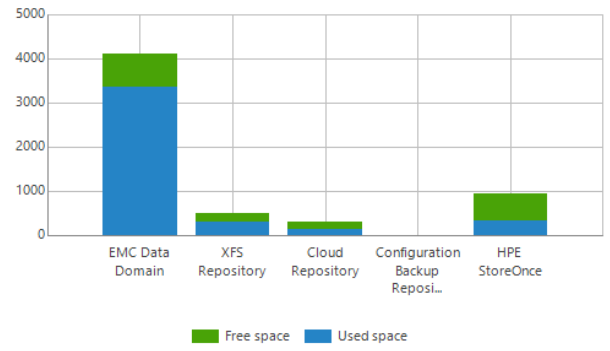
Report Parameters

Scope:	Backup Infrastructure
Space utilization threshold:	90.0 %
Safety interval:	30 days
Analyze performance data for 6 months	

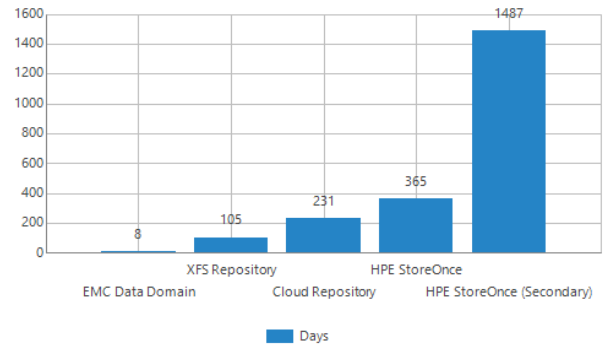
Summary

Backup Infrastructure		Physical Resources		Capacity Planning	
Number of repositories:	11	Total capacity:	28.3 TB	Min days left:	8
Number of jobs:	69	Total free space:	21.4 TB	Space required:	0.6 TB
Stored VMs and Computers:	61	Utilization ratio:	24.28%		
Stored file shares:	4				

Top 5 Utilized Repositories (GB)



Top 5 Repositories by Days Left



Report created: 11/8/2021 11:30:04 AM ((UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague)

Page: 1 of 2

veeam

Unzureichendes Datensicherungskonzept

In einem Datensicherungskonzept fließt maßgeblich, eine im Vorfeld durchgeführte Risikoanalyse, der einzelnen Services und Anwendungen ein.

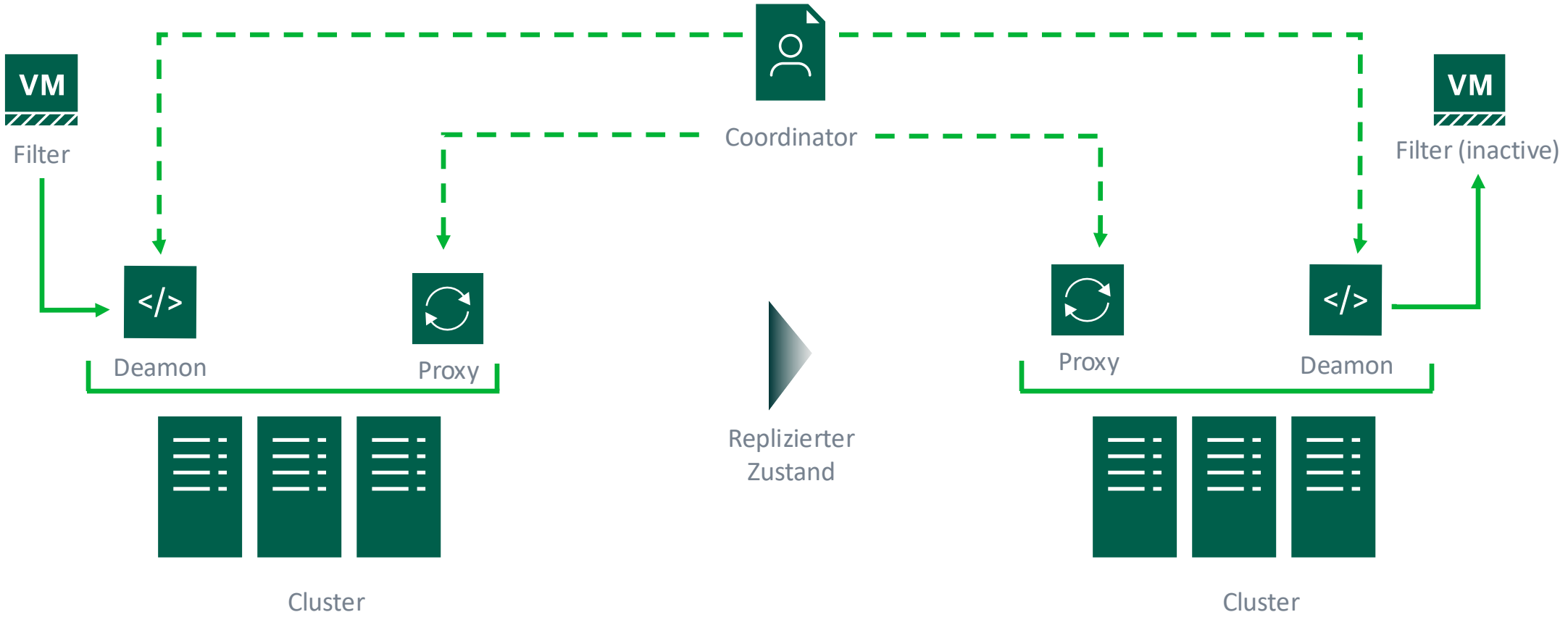
Daraus ergibt sich:

- Die RPO Zeit, Recovery Point Objective
  - Wann und wie oft wird gesichert
- Die RTO Zeit, Recovery Time Objective
  - Wiederherstellungsmethode

Unzureichendes Datensicherungskonzept

Wiederherstellungsmethoden im Veeam können unterschiedlicher RTO Zeiten genügen.

Beispiel: RPO und RTO im unteren Sekunden Bereich bei VMware



Follow us!

Join the community hub: