Eingereichte Fragen an Permapack

GBS
Gewerbliches Berufs- und Weiterbildungszentrum St.Gallen

A. Ausgangslage, allgemeine Fragen

1. Was ist der heutige Speicherbedarf?
    a. 65TB VMs, 1.2TB Exchange, 100GB OneDrive, 50GB SharePoint
2. Mit wie viel Wachstum im Jahr rechnen Sie?
    a.
3. Wie gross sind die gesamten Backups zusammen?
    a. 130TB
4. Was für eine Verfügbarkeit haben Sie?
    a.

B. Hardware, Software

1. Wird das Backup manuell oder automatisch durchgeführt? Gibt es eine zentrale Backup-Software?
    a. Backups werden automatisch durchgeführt. Es gibt für alle lokalen Quellen eine zentrale Software und für die Cloud eine eigene, zentrale Software.
2. Welche Programme oder Tools werden für Backups und deren Überwachung verwendet?
    a. Für die lokalen Backups wird «Veeam Backup & Replication» verwendet. Für die Cloud ist «Veeam for Microsoft 365» im Einsatz.
    b. Die Protokolle des Backups werden täglich geprüft, die Backups selbst gemäss. Notfallplanung. Eine automatisierte Überwachung findet nicht statt.

C. Speichermedien für Backup

1. Welche Medien werden eingesetzt?
    a. Die Backups werden auf HDDs, SSDs sowie Tapes gesichert.
2. Wie lange sind die Medien haltbar?
    a. HDDs: MTBF = 2'000'000 Stunden; erwartete jährliche Fehlerrate: 0.44%
    b. SSDs: TBW = 2'400TB; MBF = 1'500'00 Stunden
    c. Tapes: 20'000 Verwendungszyklen bzw. 30 Jahre
3. Benutzen Sie RAIDs zum Absichern der Medien und wenn ja welche/s?
    a. Backups, die auf HDDs gespeichert werden, sind mittels RAID 5 geschützt. Backups auf SSDs sind mittels RAID 6 geschützt.
4. Welche Speichermedien werden für die Backups genutzt, und warum wurde diese Wahl getroffen? (Festplatten, SSDs, Magnetbänder, Cloud-Lösungen)
    a. Die Backups werden auf HDDs, SSDs sowie Tapes gesichert.
    b. Backups werden zuerst auf SSDs gespeichert, um eine schnelle Datensicherung sowie Wiederherstellung zu ermöglichen. Die Backups werden anschliessend auf HDDs kopiert um langfristig mehr Daten günstiger (im Vergleich zu SSDs) zu lagern. Zum Schutz vor Hacker-Angriffen sowie anderweitigen Störungen, werden alle Backups auf Tapes ausserhalb der Serverräume gelagert.
5. Gibt es ein "Air-Gapped"-Backup oder andere spezifische Maßnahmen, um sicherzustellen, dass Backups nicht von Ransomware verschlüsselt oder gelöscht werden können?
    a. Alle Backups werden täglich auf Tapes geschrieben und aus den Serverräumen entfernt und an einem gesicherten Ort aufbewahrt.

D. Bedrohungslage

1. Gegen welche Bedrohungen ist ihr Backup geschützt?
    a. Hackerangriffe
    b. Brände und andere lokale (auf Gebäude beschränkte) Katastrophen
    c. Zugriff durch unbefugte Personen / Personal
2. Wie wird sichergestellt, dass die Backups vor Cyberangriffen oder Ransomware geschützt sind?
    a. Tapes werden zügig nach der Nutzung aus den Serverräumen entfernt
    b. Die Nutzung der Backup Software erfordert MFA
3. Welche Massnahmen zur Datensicherheit wurden ergriffen?
    a. Backups werden auf drei verschiedenen Systemen gespeichert (2x NAS, 1x Tape). Die NAS-Systeme arbeiten mit einem RAID.
4. Besitzen Sie ein Notstromkonzept?
    a. Aufgrund der Tätigkeiten der Firma hat sich die Geschäftsleitung gegen ein Notstromkonzept, dass über USVs hinausgeht, entschieden.
5. Wie wird sichergestellt, dass Backups auch außerhalb der Unternehmensstandorte verfügbar sind, falls die Hauptinfrastruktur ausfällt?
    a. Backups befinden sich online in beiden Serverräumen, Tapes werden in einem Tresor gelagert.

E. Backup, Archivierung

1. Welche Arten von Daten werden gesichert?
    a. Alle Server und darauf abgelegte Daten. Aus der Cloud werden Exchange, OneDrive und SharePoint gesichert. Teams nutzt die anderen Cloudfeatures und wird so indirekt mitgesichert.
    b. Daten, die lokal (im C:\) abgelegt werden, werden nicht gesichert. Das Benutzerprofil und somit u.a. der Desktop werden auf einen Server umgeleitet.
2. Wie lange dauert ein Vollbackup?
    a. Eine Vollsicherung findet nur bei der Ersten Sicherung statt. Diese sind bereits einige Jahre her. Vermutlich 3 bis 4 Tage.
3. Wann erfolgen Ihre Backups?
    a. In der Regel zwischen 19:00 Uhr und 02:00 Uhr.
4. Wird das Großvater-Vater-Sohn-Prinzip (GVS) verwendet oder ein anderes Rotationssystem?
    a. Korrekt, wir wenden das GVS-System an.
5. Welches Wechselschema benutzen Sie und wie lange kann man die Daten zurückverfolgen?
    a. Tapes werden täglich entfernt und in Ihren Gruppen (Tages- bzw. Wochenband) rotiert.
    b. Wir können bis zu 10 Jahre alte Daten wiederherstellen.
6. Welche Backup-Strategie verwendet Permapack AG? (z.b. inkrementelle, differentielle oder vollständige Backups)
    a. Wir verwenden inkrementelle Backups mit synthetischen Full-Backups.
7. welche Faktoren beeinflussen die Wahl der Strategie?
    a. Optimale Nutzung des vorhandenen Speicherplatzes
    b. Empfehlungen aufgrund von Erfahrungswerten des damaligen Dienstleisters
8. Wie lange werden die Backups aufbewahrt, und gibt es eine spezielle Aufbewahrungsstrategie? (z. B. tägliche, wöchentliche, monatliche und jährliche Aufbewahrung)

   a. Server Wichtig: 14 Tage; Server normal: 7 Tage
   b. Langzeitsicherungen der obigen Server: mindestens die letzten 7 Tage, 4 Wochen, 12 Monate und 1 Jahr
   c. Tapes mit den obigen Backups mindestens 10 Jahre
9. Wie oft werden Backups erstellt und wo werden sie gespeichert? (lokal, in der Cloud, externes Rechenzentrum?)
   a. Backups werden täglich erstellt und lokal gespeichert.
10. Verwendet Permapack AG ein mehrstufiges Backup-System? Falls ja, wie sieht der Ablauf aus? (z.b. Kombination aus NAS und Magnetbändern?)
   a. Backups werden zuerst auf einer NAS basierend auf SSDs für bis zu 14 Tage gesichert. Diese werden zeitgleich auf eine NAS mit HDDs kopiert. Auf diesem NAS werden diese bis zu einem Jahr gelagert.
   b. Gleichzeitig werden die Backups auf Tapes geschrieben und gemäss GVS-Konzept rotiert (siehe Frage 4).
11. Wie wird sichergestellt, dass Backups korrekt sind, besonders wenn Datenbanken noch laufen?
   a. Die Backupsoftware ist angewiesen Die VMs «Application aware» zu sichern. So kann diese mit den speziellen Anwendungen (u.a. Datenbanken) interagieren und in einen konsistenten Zustand setzen, bevor das Backup durchgeführt wird.
12. Sind die Backups Datenschutzkonform abgespeichert?
   a. Ja, Backups sind im internen Register für Schützenswerte Daten erfasst und entsprechend beschrieben. Der Zugang (virtuell sowie physikalisch) ist auf ein Minimum eingeschränkt und dokumentiert. Mitarbeiter, die mit Backups arbeiten sind entsprechend geschult und auf die Sensitivität des Backupinhalts hingewiesen.
13. Werden die Medien unter bestimmten Konditionen aufbewahrt?
   a. Tapes werden in einem kühlen und trocknen Tresor aufbewahrt.
14. Besitzen Sie eine Datenträgerkontroll Protokollierung?
   a. Der aktuelle Standort der Tapes sowie die Resultate der Restore-Tests werden digital protokolliert.
15. Werden die Daten von Produktionsanlagen (z. B. Maschinensteuerungen, Prozessdaten) separat gesichert
   a. Alle Produktionsanlagen, von denen die internen Betreiber ein Backup wünschen oder wir ein Backup für nötig erachten, wird auf einer zentralen VM gesichert und zusammen mit allen anderen VMs gesichert.
16. Welche Maßnahmen gibt es, um die Sicherheit und den Schutz der Backups zu gewährleisten? (Verschlüsselung, Zugriffsbeschränkungen, Firewalls)
   a. Zugriff auf die Software, sowie physischen Zugang zu den Backups ist nur einer geschulten Gruppe von Personal möglich
   b. Die Isolation des Backups steht zusammen mit der Isolation von anderen Netzwerken auf dem Projektplan
17. Welche Verschlüsselungsmethoden (hardware- und/oder softwarebasiert) setzen Sie ein, um die Datensicherheit Ihrer Backups zu gewährleisten, und wie verwalten Sie die Schlüssel?
   a. Die Daten werden verschlüsselt an das Backupsystem übertragen.
   b. Die Backups selbst sind nicht verschlüsselt
18. Wie gehen Sie in Ihrem System mit der Versionierung von Backups um, um Datenkorruption oder versehentliche Überschreibungen zu vermeiden?

   a. Das Backupsystem verwaltet die Versionierung und die eigentlichen Backupdateien selbst. Nutzer der Software sind angewiesen manuelle Vorgänge auf einem eigenen Laufwerk durchzuführen, um das Backupsystem nicht zu stören.
   b. Datenkorruption wird mittels Selbsttest der Backupsoftware sowie jährlichen Restore Tests erkannt.
19. Welche Strategien verfolgen Sie, um den Speicherplatzbedarf Ihrer Backups effizient zu managen, ohne die schnelle Wiederherstellbarkeit zu beeinträchtigen?
   a. Die Backups werden von der Storage bereits komprimiert / depubliziert. Die Backupsoftware kann dies ebenfalls. So wird im Produktivsystem sowie bei den Backups Platz gespart.
20. Wie lang werden die Daten archiviert?
   a. Onlinebackups sind bis zu einem Jahr verfügbar. Tapes werden mindestens 10 Jahre gelagert.
21. Gibt es konkrete Pläne oder Projekte zur Verbesserung der aktuellen Backup- und Restore-Strategie, beispielsweise durch den Einsatz neuer Technologien oder Automatisierungen?
   a. Das Backup-Netzwerk wird in naher Zukunft isoliert. Zudem wird eine WORM-Storage ins Backupkonzept aufgenommen.
22. Wird die 1-2-3-Regel für Backups angewendet? Wenn ja, wie wird das gemacht?
   a. Nicht komplett. Es werden zwar drei Kopien angefertigt und zwei verschiedene Speichermedien eingesetzt. Bis jetzt hat es die Geschäftsleitung nicht für nötig erachtet, Backups extern zu lagern. Eine Trennung der Gebäude reicht aktuell aus.
23. Welche Herausforderungen oder Schwierigkeiten gibt es bei der aktuellen Backup- und Restore-Strategie?
   a. Abgesehen von kommenden Projekten (Siehe Frage 21), sind uns keine Herausforderungen bekannt die gelöst werden müssen.
24. Welche konkreten Schritte sind bei einem Datenverlust vorgesehen, und gibt es dokumentierte Wiederherstellungsprozesse mit festgelegten RTO- (Recovery Time Objective) und RPO-Zielen (Recovery Point Objective)?
   a. Der einfache Wiederherstellungsprozess (eine VM / eine Datei wiederherstellen) ist nicht dokumentiert. Mitarbeiter, die dies können müssen sind entsprechend geschult. Grössere Szenarien sind gem. Notfallkonzept dokumentiert.
   b. Die RTO für kleine Vorfälle beträgt max. 4 Stunden. Bei grösseren Störungen bewegt sich die RTO zwischen 4 und 11 Tagen. (inklusive Störungsanalyse / Analyse durch externe Spezialisten für Hacking-Vorfälle). Systeme, die erst nach 11 Tagen wieder online sind, sind unwichtige Randsysteme, die nicht Zeitkritisch sind (Update-Cache Server, etc.)
   c. Wir unterteilen die RPO in zwei Kategorieren (kleine Störungen und Verlust eines RZ). Bei kleinen Störungen bewegt sich die RPO zwischen 0.5 und 24 Stunden. Beim Verlust eines RZ ist diese immer 1 Woche.
25. Gibt es eine Archivierungsstrategie für langfristige Aufbewahrung von Backups
   a. Die Strategie ist recht simpel (keep it simple, stupid): Das letzte Wochenband eines Monats wird gemäss Monatsrotation gelagert. Sollte das Monatsband das letzte Band des Jahres sein, wird es aus der Rotation entfernt und für mindestens 10 Jahre gelagert.

F. Restore

1. Gab es bereits einen Vorfall, bei dem ein Backup wiederhergestellt werden musste? Wenn ja, hat der Restore ohne Probleme funktioniert?

   a. Bis jetzt waren das kleinere Vorfälle (Dateien / Ordner gelöscht und Monate später bemerkt). In diesem Fällen hat der Restore problemlos funktioniert.
2. Was passiert, wenn ein Backup beschädigt oder unvollständig ist?
   a. Dies ist immer Situationsabhängig. Wird beim Erstellen des Backups eine Störung erkannt / bemerkt, wird das Backup, wenn möglich wiederholt.
   Wird bei einem geplanten Testlauf eine Störung des Jahresbands erkannt, wird ein anderer Monat als Jahresband festgelegt – insofern das Backup nicht wiederholt werden kann.
   Unvollständige Backups werden so schnell wie möglich nachgeholt.
   Es ist zu erwähnen, dass bis jetzt keine Fehlerhaften Backups gefunden wurden und unvollständige Backups höchst selten sind.
3. Welche Snapshot-Technologien werden für schnelle Wiederherstellung eingesetzt?
   a. Im Bezug auf Wiederherstellung bestehen zwei Möglichkeiten: Die VM existiert noch und die Backupsoftware stellt nur die auf der Storage veränderten Blöcke wieder her (Veeam quick rollback). Existiert die VM nicht mehr, kann die VM direkt aus dem Backuprepository gestartet werden und im Hintergrund auf die produktive Storage migriert werden (Veeam Instant Recovery).
4. Wie schnell können Sie im Notfall eine Wiederherstellung der Daten durchführen?
   a. Im Katastrophenfall dauert die Wiederherstellung inklusive Analyse durch externe Spezialisten (im Falle eines Hackerangriffs) bis zu 11 Tage
5. Gibt es ein definiertes Disaster-Recovery-Konzept und Notfallpläne?
   a. Ja diese gibt es und sind vorallem auf Szenarien ausgelegt, bei denen beide RZs ausfallen. Sollte nur ein RZ ausfallen übernimmt das verbleibende RZ automatisch die zusätzliche Last.
6. Gibt es einen Plan, welche Systeme nach einem Totalausfall zuerst wieder hochgefahren werden?
   a. Ja, ein solcher Plan existiert. Im groben gilt folgende Reihenfolge:
   Infrastrukturrelevante Systeme, primäres ERP, sekundäres ERP, primäre Applikationen der Fachabteilungen und anschliessend alle Randapplikationen.
7. Gibt es eine genaue Zeitvorgabe für die vollständige Wiederherstellung aller Systeme, z. B. nach einem Rechenzentrumsausfall? Welche Ressourcen (z. B. Cloud, Notfallserver) stehen zur Verfügung, um dies zu ermöglichen?
   a. Die Zeitvorgabe richtet sich aktuell nach der technischen Machbarkeit der aktuellen Backupsysteme. Dieses Zeitfenster wurde durch die Geschäftsleitung abgesegnet.
   b. Im Katastrophenfall steht vermutlich die Cloud noch zur Verfügung, dies bedeutet, dass das primäre ERP sowie E-Mails und Teams noch verfügbar sind. Zusätzlich gehen wir davon aus, dass die Telefonanlage unberührt bleibt, da Permapack keine VoIP Telefone einsetzt. Ersatzhardware steht nur bedingt bereit und kann nicht verwendet werden und die gesamte Infrastruktur darauf laufen zu lassen. Wir gehen davon aus, dass – ohne Hackerangriff – höchstsens eines der Rechenzentren Hardwaremässig betroffen sein wird.
8. Welche IT-Systeme haben Priorität beim Wiederanlauf nach einem kompletten Ausfall?
   a. Siehe Frage 6.
9. Wie oft werden die Backup- und Wiederherstellungsprozesse getestet, um ihre Zuverlässigkeit zu gewährleisten?
   a. Die Backups werden ein Mal im Jahr getestet. Sollte im Verlauf des Jahres ein Restore vom Band durchgeführt werden, würde das ebenfalls im Testprotokoll aufgenommen werden.

10. Welche Herausforderungen gab es in der Vergangenheit bei der Datenwiederherstellung und wie wurden sie gelöst?
    a. Uns sind in den letzten 8 Jahren keine grösseren Herausforderungen aufgefallen.

G. Kosten

1. Wie gross sind die Kosten?
    a. Software: ca. 15k CHF jährlich
       Hardware: ca. 45k CHF ohne Wartungsverträge
2. Wie hoch sind die Kosten für Backup-Medien wie Magnetbänder oder Festplatten? (Laufende Kosten für Speicherplatz, Anschaffungskosten)
    a. Kaufpreis pro Tape: ca. 90 CHF
    b. Kaufpreis der eingesetzten HDDs (pro HDD): ca. 500 CHF
    c. Kaufpreis der eingesetzten SSDs (pro SSD): ca. 600 CHF
    d. Da keine Cloud im Einsatz, keine laufenden Kosten für Speicherplatz. Die Abschreibung erfolgt nach einer Mischrechnung und ist daher nicht aussagekräftig genug für die laufenden Kosten des Backupsystems.

H. Organisation

1. Wie sind die Rollen und Verantwortungsbereiche bei Ihnen aufgeteilt?
    a. Der Bereich Infrastruktur der IT betreut das Backupsystem vollständig (tägliche Arbeiten, Restores, Weiterentwicklung, Pflege, etc.).
2. Wer ist verantwortlich für die Überwachung und Wartung der Backups?
    a. Der Bereich Infrastruktur der IT
3. Werden Schulungen zum Thema Backup für die Mitarbeiter eingesetzt?
    a. Da Backups sowie Restores nur durch die IT durchgeführt werden, werden nur neue Mitarbeiter im Bereich Infrastruktur beim Eintritt entsprechend geschult.
4. Testen Sie regelmässig Ihr Backup?
    a. Ja, jährlich. Diese Tests werden auch protokolliert – auch im Bezug auf Performance.
5. Werden regelmäßige Tests der Wiederherstellung durchgeführt, um die Funktionsfähigkeit zu überprüfen?
    a. Siehe Frage 4
6. Welche Maßnahmen werden ergriffen, um Datenverluste durch defekte oder veraltete Backup-Medien zu vermeiden? (z. B. regelmäßige Tests, Austausch alter Speichermedien)
    a. Festplatten und SSDs befinden sich in einem RAID und werden bei einer Störung ohne Datenverlust ausgetauscht. Tapes werden ausgetauscht, wenn diese als «defekt» erkannt werden. Tapes die sich im Jahresband-Tresor befinden werden nur nach einem Jahr nochmals getestet. Ausfälle nach dieser Zeit werden nicht erfasst / erkannt / behoben.
7. Wie schnell kann auf einen Serverausfall reagiert werden?
    a. Das interne SLA schreibt eine Reaktionszeit während der Arbeitszeit von max. 1 Stunde vor. Ausserhalb der Arbeitszeiten gilt eine Reaktionszeit von 4 Stunden.