Backups in Unternehmen

Warum Veeam ungeeignet für die meisten ist/n- Printout von blog.jakobs.systems

Tomas Jakobs

29 Dezember 2024

Inhaltsverzeichnis

Warum ist das Geschäftsmodell Ransomware so erfolgreich? Wie schaffen es Kriminelle Daten zu entwenden, zu verschlüsseln und häufig auch die Datensicherungen zu vernichten? Laut repräsentativer Umfrage der BITKOM in den vergangenen 12 Monaten bei 60% der Unternehmen in Deutschland.[1]

Ein kurzer Exkurs in diese Thematik, in meine Arbeit und wie ich einem Unternehmen helfen konnte, 17.000,- EUR zu sparen. Wie immer gilt, kein Anspruch auf Vollständigkeit und Allgemeingültigkeit. Your milage may vary.

Kaputte Datensicherungskonzepte

Die Antwort liegt in den Datensicherungskonzepten. Eingebettet im ISMS und angeknüpft an Notfall- und Kontinuitätsplänen. Aus der eingangs genannten BITKOM Umfrage ist zu entnehmen, dass bei 60% der Betroffenen das genau Totalausfälle sind:

> Vier von zehn (40 Prozent) der betroffenen Unternehmen konnten ihre Daten selbst wiederherstellen, 10 Prozent haben sie ohne Lösegeldzahlung von den Tätern zurückbekommen.

Ohne in die Untiefen der verschiedenen Zertifizierungsnormen einzutauchen beantwortet ein Konzept immer die nachfolgende Fragen:

- Welche RPO (Recovery Point Objective) und RTO (Recovery Time Objective)[2] sind definiert?
- Lassen sich diese bei Totalausfall mit der bestehenden Technik und Personal auch erreichen?
- Existieren vom Regulärbetrieb getrennte Offline- bzw. Offsite-Sicherungen?
- Werden Abhängigkeiten und Reihenfolgen berücksichtigt?
- Erfolgt in regelmäßigen Abständen eine methodische Prüfung?
- Sind Änderungen transparent und nachvollziehbar?

[1] https://bitkom-research.de/news/mehr-als-die-haelfte-der-unternehmen-werden-opfer-von-ransomware-attacken

[2] https://de.wikipedia.org/wiki/Disaster_Recovery

Mangelhafte Backupsoftware

Spätestens bei den letzten beiden Fragen wird deutlich, es existiert keine Standard-Software, die Antwort geben kann.

Auf der einen Seite gelangt Software immer mehr automatisiert mit CI/CD[3] Pipelines, Deploy- und Rollouts-Workflows auf die Systeme. Bei Sicherung und Wiederherstellung jedoch wuseln Administratoren erfahrungsgemäß manuell durch mehr oder minder miserable Dialoge.

Abhängigkeiten und Reihenfolgen werden allein durch die “Logik” des Administrator bestimmt. Was meine ich damit? Es ist zum Beispiel doof, wenn zeitgleich alle DNS Server offline gesichert und somit nicht verfügbar sind. Mehr doof ist es, wenn zwei Monate später ein anderer Admin fragt, warum der zweite DNS fehlt und meint, diesen schnell mit in den Job zu schubsen.

Die wenigsten nutzen APIs und Scripting-Integrationen, sofern von einer Backupsoftware überhaupt angeboten. Wie kann ohne Automatisierung eine Prüfung methodisch und regelmäßig erfolgen? Und von Skalierung will ich gar nicht erst anfangen.

Bemerkenswert ist, dass Sicherungsjobs selbst keine Audit- oder Changelogs aufweisen. Welcher Administrator hat was, wann, wo gemacht bleibt bei Veeam & Co unbeantwortet. Wie will ein Verantwortlicher und Nicht-Admin wissen, ob eine bestimmte VM noch Bestandteil einer Sicherung ist oder zwischenzeitlich gegen was anderes getauscht wurde?

So sicherte ein mir persönlich bekanntes Unternehmen fast ein Jahr lang nicht die VM des kritischen ERP-Systems sondern die Entwicklungsumgebung des externen Dienstleisters. Die Verwechselung wurde von einem Admin während einer “Bereinigung” verursacht und fiel niemanden auf. Erst als die Entwicklungs-VM final beseitigt wurde, wunderten sich alle, warum die täglichen Status-Mails nicht mehr grün sind.

Backupsoftware wird zunehmend selbst zum Problem. Proprietäre Blackboxen mit unbekannter Arbeitsweise werden zentral eingerichtet und können über bewusst eingezogene Segmente und Trennungen hinweg in kritische Bereiche hineinwirken.

Zugleich sammeln sich an diesem Single-Point-of-Failure[4] per Powershell-Skript einfachst auslesbare Zugangsdaten.[5] Zunehmender Online-Zwang und intransparente Datenabflüsse in Gestalt von Telemetrie gesellen sich als Herausforderungen dazu.

---

[3] https://en.wikipedia.org/wiki/CI/CD

[4] https://en.wikipedia.org/wiki/Single_point_of_failure

[5] https://github.com/sadshade/veeam-creds

```
59    "Here are some passwords for you, have fun:"
60
61    #Decrypting passwords using DPAPI
62    $rows | ForEach-Object -Process {
63            $EnryptedPWD = [Convert]::FromBase64String($_.password)
64            $ClearPWD = [System.Security.Cryptography.ProtectedData]::Unprotect( $Enrypted
65            $enc = [system.text.encoding]::Default
66            $_.password = $enc.GetString($ClearPWD)
67    }
68
69    Write-Output $rows | FT | Out-string
```

Abbildung 1: Veeam-Credentials per Powershell auslesen

Herausforderungen nicht verstanden

Administratoren arbeiten oft mit Methoden der 80er und ignorieren den Fortschritt der vergangenen Jahrzehnte. Obwohl die Anzahl der Server steigt, sehe ich immer noch ein manuelles Anmelden auf Servern. Unabhängig von ideologischen Diskussionen “Linux oder Windows”, “Konsole oder GUI” ist das einfach nur Pfui!

Skalierung bedeutet nicht, mehr Personal einzustellen sondern mehr und vor allem besser zu automatisieren. Kristian Köhntopp zeigte vor 9 Jahren in seiner Präsentation “Go Away Or I Will Replace You With A Very Little Shell Script” wie unproduktiv und gefährlich ein manuelles “Rumklettern” auf Servern ist:[6]

> Wenn man auf einen Rechner klettern muss, um etwas nachzuschauen, ist offensichtlich das Monitoring kaputt. Wenn man auf einen Rechner klettern muss, um etwas zu ändern, ist offensichtlich die Automatisierung kaputt und vermutlich, hoffentlich, nicht nur die eine Kiste kaputt, sondern alle andern auch und zwar hoffentlich gleich.

Überall wo Verfügbarkeiten garantiert werden müssen, weil Unternehmen und Existenzen davon wirtschaftlich abhängen, ist eine Automatisierung zwingende Voraussetzung.

Wir nutzen “Veeam” höre ich oft. Schön, das Problem leider nicht verstanden. Ich befürchte, die Geschäftsmodelle mit dem mehrfachen Abkassieren werden noch nicht einmal bemerkt: Teure Lizenz-Abos proprietärer Software auf der einen, Lösegeld auf der anderen Seite. Aber

[6] https://media.ccc.de/v/froscon2015-1500-

der Support bei Veeam sei so gut. Welcher Support? Kein Callcenter-Agent und Nicht-Admin am anderen Ende einer Telefonleitung, Chats oder EMail hilft Dir, wenn alles steht und die Backups futsch sind. Akuter Fall von Stockholm-Syndrom.[7]

GitOps-Lösungsbeispiel

Aus dem DevOps[8] heraus entwickelt bedeutet der Begriff GitOps den Betrieb einer Infrastruktur mit Hilfe einer Git[9] Versionskontrolle. Die “Single Source of Truth”[10] im Operations für Infrastruktur, Servereinrichtung, Anpassung von Softwarepaketen bis zu den automatisierten Prozessen mit Ihren Skripten stehen da transparent und nachvollziehbar.

Letztes Jahr stand ein mittelständisches Unternehmen vor der Fragestellung, ob es weiter gewillt ist, für einen kleinen HyperV Cluster aus zwei Nodes, hohe Summen auszugeben. Zur Disposition standen 17.000,- EUR.

[7] https://en.wikipedia.org/wiki/Stockholm_syndrome

[8] https://en.wikipedia.org/wiki/DevOps

[9] https://git-scm.com/

[10] https://en.wikipedia.org/wiki/Single_source_of_truth

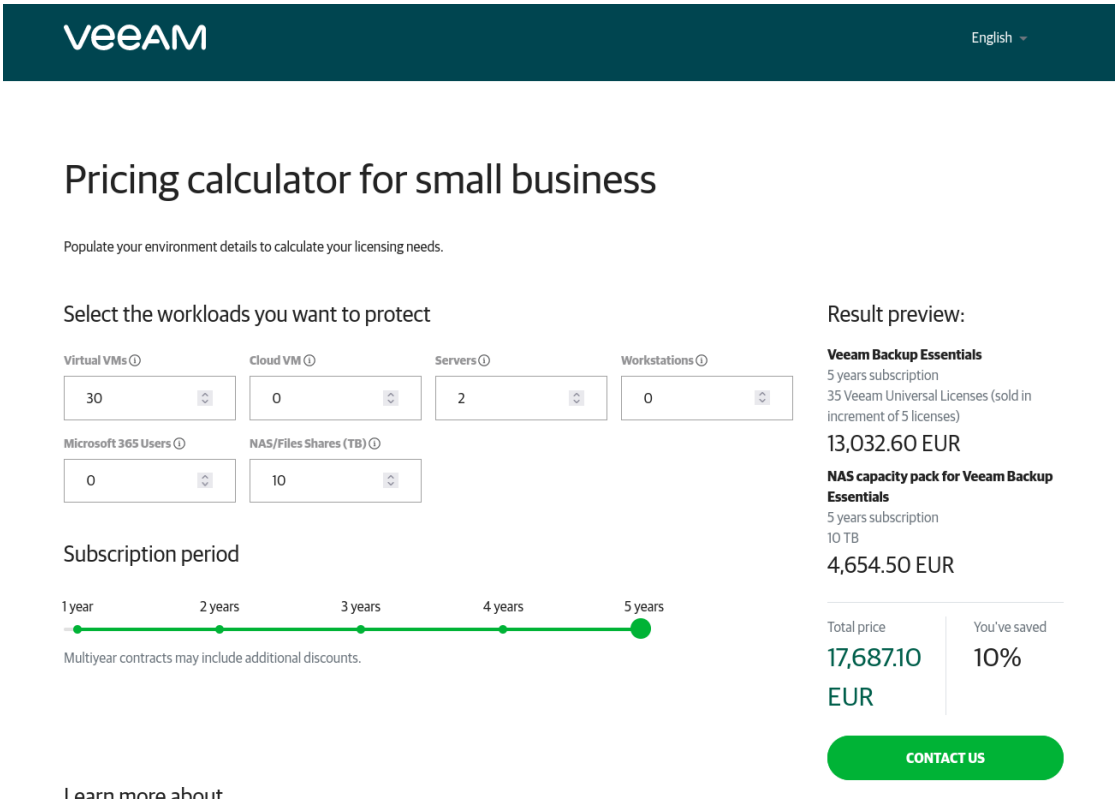

Abbildung 2: Screenshot Veeam Kosten-Kalkulation

Für vollständige, tägliche Sicherungen von allen VMs, ergänzt durch mittwöchentliche und wöchentliche Auslagerungen auf ein anderes Storage und externe USB-Medien bedarf es keiner proprietären Software.

Mit einem Bruchteil der Kosten laufen heute alle Sicherungen kontrolliert von einem nur intern erreichbaren Forgejo-Server.[11] Jedes Node im Cluster pullt automatisiert das Repo mit seinen Skripten für Datensicherungen und führt diese aus.

Positiver psychologischer Nebeneffekt für jeden Geschäftsführer: Es tut gut, die ganze Firma in der Hand zu halten und jederzeit an einem beliebigen Rechner alles wieder hochzufahren.

[11] https://forgejo.org/

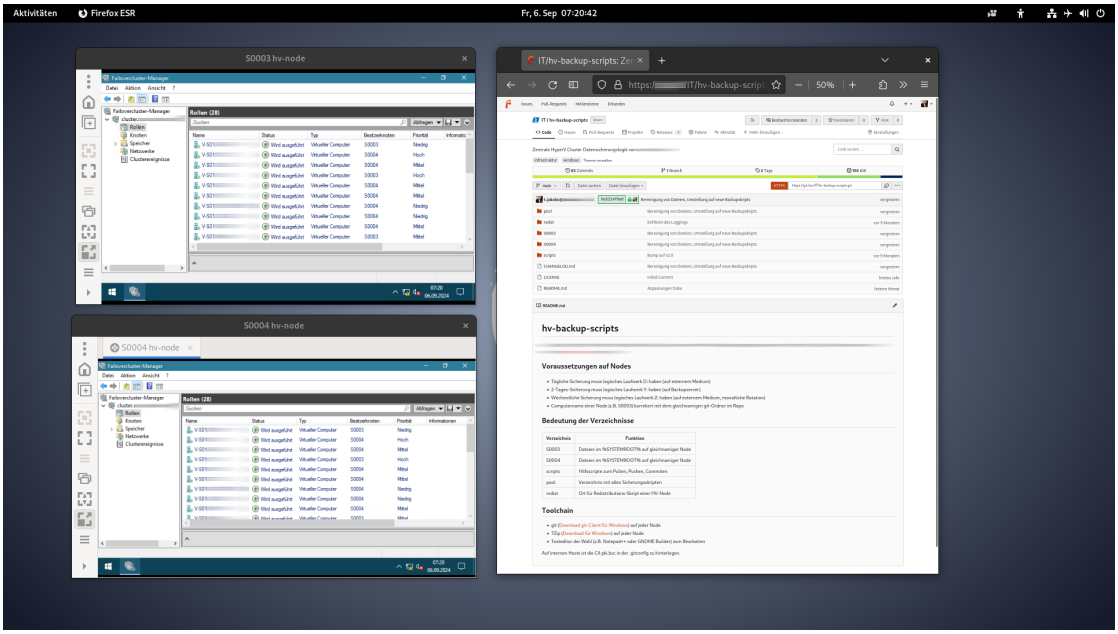

Abbildung 3: Screenshot 2 Nodes und Git-Repo

Seitdem haben sich weitere Repositories hinzu gesellt. Von den vorgestellten “digitalen Zwillingen” zum Testen von Windows-Updates[12] bis zum Erstellen halbtäglicher Datenbankdumps aller Fachanwendungen. Von Bash, PowerShell, Batchfiles und Ansible-Skripten bis zu kleinen Tools und AutoIt-Programmen findet sich hier alles wieder - your milage may vary.

Fazit

Die meisten Datensicherungskonzepte halten einem Realitätsabgleich nicht stand. Administratoren wuseln vor sich her. Fehlende Automatisierung treibt die IT Kosten in die Höhe, erzeugt Fehler und technische Schulden.

Einheitliche GitOps-Workflows sind die Lösung. Die Technologie ist frei, das Konzept weder kompliziert noch schwer umsetzbar.

Es bleibt zu erwähnen, dass GitOps für Datensicherungen nur dann funktioniert, wenn im Vorfeld einige Hausaufgaben erledigt wurden. Das sind nicht weg migrierte Exchange-Blackboxen, fehlende Mailgateways, fehlende Mailarchivprogramme, nicht isolierte Netzwerksegmente

[12] https://blog.jakobs.systems/micro/20240814-digitale-zwillinge/

und leider häufig auch eine fehlende Trennung von Hypervisoren vom zu schützenden AD. Hier kommt die Fehlkonzeption von Microsoft zu Tage, dass ein HyperV-Cluster Mitglied einer Domäne sein muss. Die Kombination mit Bequemlichkeit ergibt den sprichwörtlichen Clusterfuck, wenn der letzte DC von Ransomware dahinrafft ist und der Cluster nicht mehr hochfährt.

Wichtigste Voraussetzung für GitOps ist aber das passende Mind-Set, die Kultur. Administratoren müssen in der Lage sein, Probleme systematisch zu betrachten und frei von Ideologien programmiertechnisch lösen.

In diesem Sinne,
Euer Tomas Jakobs