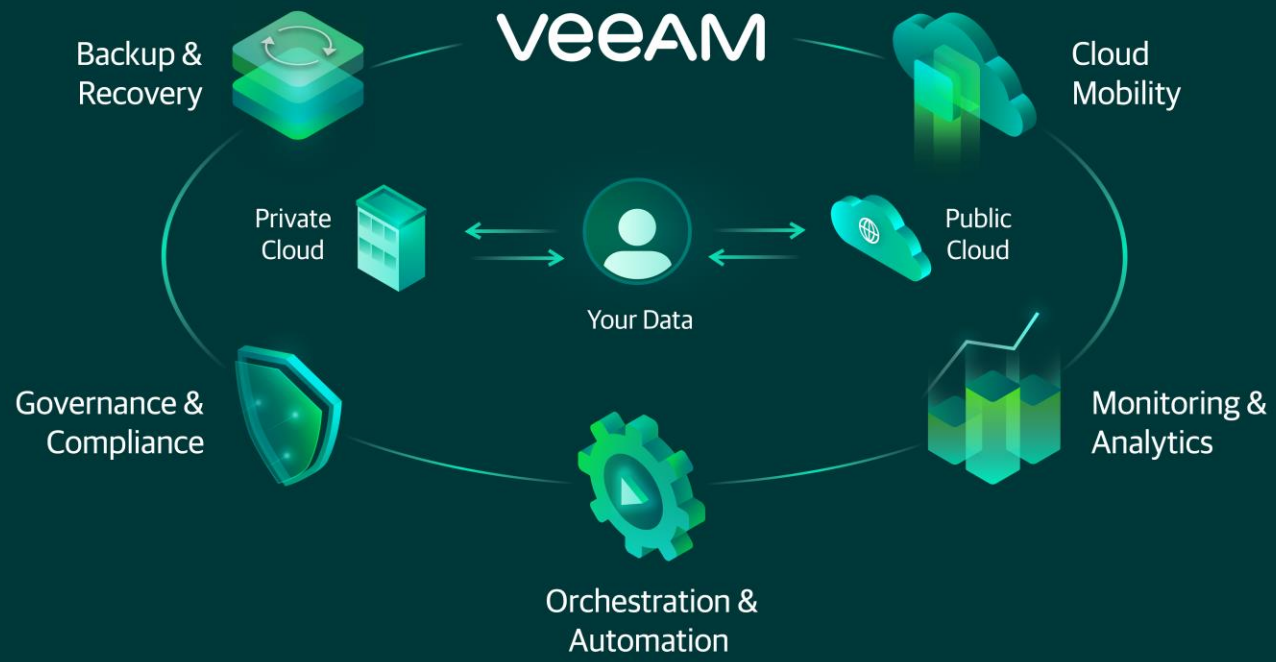
3 strategie per il Recovery da Ransomware nei giorni del Remote Working

Giampiero D. Cannavo'
Regional Alliance Manager Southern EMEA
Giampiero.Cannavo@Veeam.com

Cloud Data Management



Gestione e protezione efficaci dei dati, su infrastrutture on-premises e cloud
Utilizzo delle copie dei dati per innovazione e test di verifica

Il backup è davvero così «noioso»?

Il backup esiste da quando esiste l'IT…
ma ci sono state significative evoluzioni negli ultimi anni

Scenari	Sfide

Anche le minacce si evolvono…

Malware sempre più «intelligenti»:

- Finalità non sempre/solo distruttive
- Tecniche di occultamento, malware «dormienti»
- Esfiltrazione dati (spionaggio, sabotaggio)
- Profitto da «riscatto» per dati crittografati
- Attacchi proattivi contro antivirus e backup

POST REPLY | Search this topic…

Yes, Ransomware can delete your Veeam backups.

by **kbossak** » Mon Mar 06, 2017 6:05 pm

https://forums.veeam.com/veeam-backup-replication-f2/yes-ransomware-can-delete-your-veeam-backups-t41500.html

3 strategie per il Recovery da Ransomware nei giorni del Remote Working

- Regola 3-2-1-0

La regola 3-2-1-0

Ripristina i dati in qualsiasi situazione - specialmente dopo attacchi ransomware!

3	2	1	0
copie dei dati	media diversi	dei quali off-site *	errori grazie ai test di ripristino

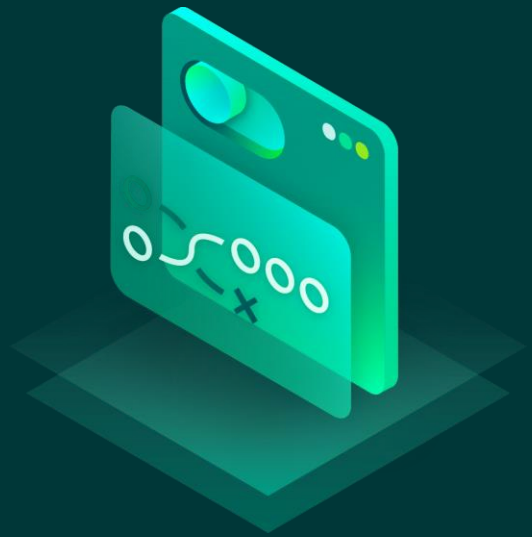
* Senza dimenticare le copie offline!

3 strategie efficaci contro il ransomware

- Regola 3-2-1-0
- Hardening di infrastruttura e servizi

Hardening

Best practices e suggerimenti per aumentare la sicurezza
delle infrastrutture Veeam Backup & Replication



- Controllo degli accessi
  - Separazione utenze amministrative
  - Accesso controllato ai sistemi (RDP, SSH, etc.)
  - Accesso controllato ai repository (attenzione a share NAS!)
- Riduzione della superficie di attacco
  - Rimozione software / servizi non essenziali
  - Separazione dei ruoli (backup server / proxy / repository…)
  - Gestione efficace di aggiornamenti e patch
  - Diversificare repository / file system (Windows, Linux, appliance di deduplica…)

3 strategie efficaci contro il ransomware

- Regola 3-2-1-0
- Hardening di infrastruttura e servizi
- Monitoraggio, formazione utenti

Monitoraggio

Visibilità immediata sulle potenziali minacce

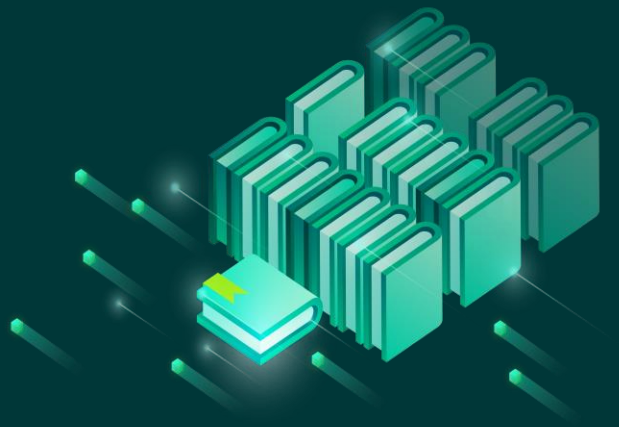
- Soluzioni di sicurezza perimetrale, ispezione traffico, analisi
  - Tentativi di accesso non autorizzati
  - Codice malevolo
  - Individuazione sistemi non aggiornati / non sicuri
  - Analisi "sandbox" di mail / allegati / URL
  - Audit attività utente
  - DLP (Data Loss Prevention)

Monitoraggio

Funzionalità incluse in Veeam ONE:

- Allarme "Potential ransomware activity"
  - Analisi pattern anomali CPU, I/O e traffico di rete
- Allarme "Suspicious increment size"
  - Crescita anomala del backup incrementale
- Veeam Intelligent Diagnostics
  - Analisi dei log Veeam Backup & Replication per rilevare anomalie, errate configurazioni, problemi

Formazione utenti



Gli utenti sono i principali vettori per le minacce informatiche

- Promuovere best practices
  - Password policy
  - Corretto salvataggio dei dati
  - Condivisione sicura dei dati
  - Attenzione a mail ed allegati
- Strumenti di simulazione ed assessment
  - Valutazione minacce phishing (KnowBe4, GoPhish…)
  - Valutazione minacce ransomware (RanSim, etc.)