Traditionel backup sikrer ikke længere virksomhedens data

Mange IT-ansvarlige opdager for sent, at de ikke er ordentligt beskyttet mod moderne cyberkriminalitet. Det kan blive uhyggeligt dyrt og i de værste tilfælde true virksomhedens mulighed for at overleve.

Din mobiltelefon ringer mistænkeligt tidligt den morgen. Det er salgschefen, og han er ikke i særlig godt humør. Både CRM-systemet og lagerstyringen er nede. Alt salg og distribution kommer til at ligge stille, indtil systemerne kører igen. Du skynder dig ud ad døren for at komme ind på jobbet og få det fixet.

På vejen bliver du ringet op af direktøren. Han fortæller, at mailserverne tilsyneladende er låst, og i baggrunden kan du høre en desperat stemme råbe, at webshoppen heller ikke virker.

På kontoret er stemningen ret anspændt. Hvad pokker er der galt? Du når lige at tænke, at det er godt, at I har backup af alle data i en krisesituation som denne. Så går det op for dig, at det ikke er en krise. Det er et mareridt.

I er nemlig udsat for et angreb, hvor cyberkriminelle er brudt gennem jeres firewall og via ransomware har låst og krypteret jeres data. Nu forlanger de en stor løsesum for at låse op igen - og det allerværste er, at hackerne også har låst alle jeres backupkopier.

Backupløsningen er også under angreb

”Tidligere gik cyberkriminelle efter forretningens primære produktionsdata, men nu er backup-filer også et udsat mål for ransomware-angreb mod virksomheder, der ikke har sikret sig med en tidssvarende backup-løsning”, siger Claus Munch, Head of Backup hos GlobalConnect i Danmark, og fortsætter:

”I dag er data altafgørende. Langt de fleste virksomheder er dybt afhængige af konstant adgang til deres data for at holde forretningen i gang. Hvis virksomheden ligger underdrejet, fordi nogen har kidnappet forretningskritiske data, og ovenikøbet også fået fingre i backupkopierne, koster det hurtigt en formue. I de mest alvorlige tilfælde koster det virksomheden livet”, konstaterer han.

For ikke så længe siden var en virksomhed rimeligt sikret med en traditionel dual-site backupløsning: Backup af alle data hos virksomheden selv for at sikre fuld udnyttelse af den lokale netværkskapacitet til backupkopiering og eventuel gendannelse, og så en ekstra kopi af det hele et sikret sted på en anden adresse, fx et sikkerhedscertificeret datacenter.

Nye trusler mod traditionelle løsninger

I dag har trusselbilledet ændret sig, og den traditionelle dual-sitebackup er langt fra sikker nok, vurderer Claus Munch:

“Det er et våbenkapløb mellem cyberkriminelle og backupløsninger, der er sikre nok. Heldigvis er GlobalConnect et par skridt foran her. Sammen med softwareleverandøren Veeam, som er førende på det europæiske marked indenfor backupløsninger, der garanterer hurtig gendannelse, tilbyder vi en tidssvarende backupløsning, som både beskytter effektivt mod ransomware og fejlsletninger af vigtige data”.

Løsningen hedder Veeam Cloud Connect

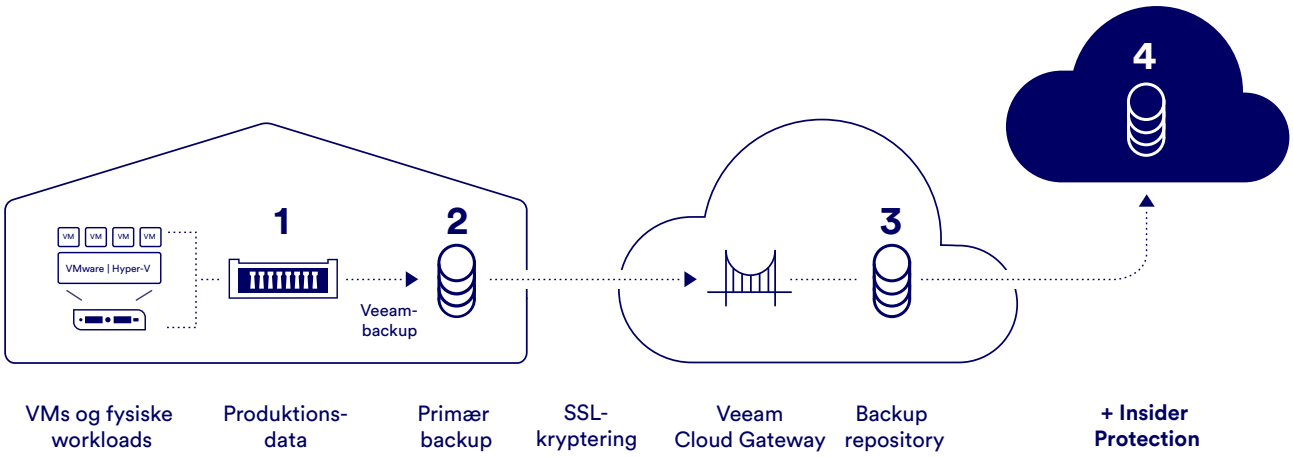
GlobalConnect er Veeam Platinum Partner og tilbyder kunder, som allerede bruger Veeam Backup & Replication, at de nemt kan tilføje løsningen Veeam© Cloud Connect, og dermed også sikre backupdata mod at blive slettet ved en fejl eller blive krypteret af cyberkriminelle, der så forlanger løsesum for at låse dem op igen.

”Vi har taget udgangspunkt i best practice og sikrer vores kunders data ved at følge 3-2-1-reglen, altså at man opbevarer tre kopier af sine data, hvoraf to kopier eksisterer (1) som produktionsdata og (2) lagres som lokal backup i virksomheden - og en tredje kopi (3) lagres i et af GlobalConnects topsikrede datacentre”, fortæller Claus Munch.

”Ved at have tre kopier, og sørge for at de ikke befinder sig samme sted, er man godt i gang – men ikke færdig - med at sikre sig mod nedbrud, fejlsletninger og hackerangreb”.

Der er stadig et sikkerhedshul tilbage. Og det hul lukker løsningen Veeam© Cloud Connect, forklarer Head of Backup hos GlobalConnect, Claus Munch.

Sådan sikrer Veeam© Cloud Connect jeres backupdata mod ransomware



1. Produktionsdata
Dine data gemmes på dit primære medie – lokalt på enten din computer eller server.

2. Primær backup
Dine primære backup-data gemmes via Veeam-backup på et lokalt backup-medie i virksomheden.

3. Backup repository
En tredje kopi lagres off-site med Veeam Cloud Connect for at sikre mod lokale ulykker og sikkerhedsbrud.

4. + Insider protection
Insider Protection beskytter dig, hvis dine øvrige backup-data kompromiteres – i lige så mange dage, du har brug for.

Hemmeligheden er den usynlige folder

”Problemet med de traditionelle backupløsninger er, at hvis først en cyberkriminel slipper gennem firewallen og ind på netværket, har han også adgang til backupkonsollen, hvor man kan kontrollere både de backupkopier, der ligger på egen lokation, og dem der er på den anden lokation, fordi den også er tilgængelig online”.

”Den mulighed fjerner Veeam© Cloud Connect, fordi løsningen automatisk genererer en kopi af alle data, som nogen sletter eller krypterer, i en særlig Insider Protection folder. Folderen er ikke synlig på vores kunders netværk og dermed heller ikke for uønskede gæster. De cyberkriminelle tror så, at de har krypteret backuppen, der i virkeligheden stadig findes ukrypteret og er placeret sikkert i den ’usynlige’ folder. Her opbevares filerne i en periode, der aftales individuelt med hver enkelt virksomhed”, slutter Claus Munch.

3 tip til tidssvarende databeskyttelse

Jeres backupdata skal også sikres

Hvis cyberkriminelle får adgang til jeres netværk, kan de kryptere alt, også backuppen, og kræve løsepenge.

En backupløsning kan ikke stå alene

Tidssvarende og altid opdateret firewall/antivirus/styresystem hører med i den samlede sikkerhedspakke.

Husk disaster recovery-planen

Er uheldet alligevel ude, kan det være afgørende for hvornår forretningen kører igen, at disaster/recovery-processen er klar.