QUICKGUIDE

Cyber Recovery

Hackeren er kanskje allerede i backupen din?

- 10 ting du skal være oppmerksom på

Dell EMC Cyber Recovery Solution

DELL Technologies

DELL Technologies PLATINUM PARTNER

serit.no

serit

Smart IT. God jobbdag.

Det er kun et spørsmål om tid før du blir utsatt for et angrep. Din backup kan være målet!

Cyber Recovery:
10 ting du skal være oppmerksom på:

1 Hackerne lister seg inn bak din «last line of defence»

Du har uten tvil følt eller opplevd den økte trusselen fra mer og mer agressive og kreative hackere. Derfor har du selvfølgelig investert i virus-scanning, firewall, multifaktorautentisering, VPN og mer. Men er det nok? Akkurat som mange av kollegene dine, kan du være i tvil.

De fleste selskaper i dag beskytter seg mot angrep utenfra med en digital mur rundt IT-systemene sine. Dessverre er dette ikke lenger tilstrekkelig, da det mest sannsynlig vil forekomme angrep som trenger gjennom muren eller starter fra innsiden. Trusselbildet har endret seg, og hackerne retter seg nå mot din «last line of defence» – backup-systemet ditt!

2 Angrep på backup-systemet kan pågå i flere måneder uten at du en gang er klar over det!

Hackere finner nye veier inn, og det som kan skje hvis de får tilgang til backupen din, er ondere enn ondt. Og like lydløst blir flere og flere av sikkerhetskopifilene smittet over lang tid uten at det blir lagt merke til på noen måte.

Når det faktiske angrepet starter etter – vanligvis etter å ha vært infisert tre til seks måneder – og det er behov for å laste ned backup-filer, viser det seg at de siste uinfiserte filene er så gamle at de stort sett er ubrukelige. Dette gir deg både ødelagte produksjonsfiler og en utdatert backup. Krisen er total

3 Passer backup-planen din til virksomheten din? Det kan være dyrt å ta feil!

Du har selvfølgelig en plan for regelmessig backup og sikring av selskapets data. Men er denne planen god nok når/hvis skaden skjer? Mengden virksomhetskritiske data øker stadig samtidig som virksometen krever at data må være tilgjengelig uansett hvor og når.
Den dagen angrepet kommer, er det din evne til å beskytte selskapets kritiske data og muligheten til raskt å gjenopprette dem som bestem mer omfanget av skaden. Og den kan som kjent være stor. Så stor at tre av fem bedriftsledere i verden ser cyberangrep som en av de største truslene mot deres virksomhet!

4 Er backup-strategien din sterk nok?

Den endrede atferden til hackerne betyr at backup-strategi bør gis høy prioritet. Du står overfor en fiende som kommer listende på tå med en ny taktikk i form av superfarlige angrep, som i likhet med andre angrep kan komme både fra utsiden og innsiden. Er din nåværende strategi sterk nok til å tåle denne typen angrep? Inntil nå har i det minste hackerne klart å omgå de vanlige systemene og komme seg inn bak forsvarslinjene.
Det beste rådet akkurat nå er derfor å forberede seg så godt som mulig på et angrep. For det kommer før eller siden – hvis det ikke allerede har startet …

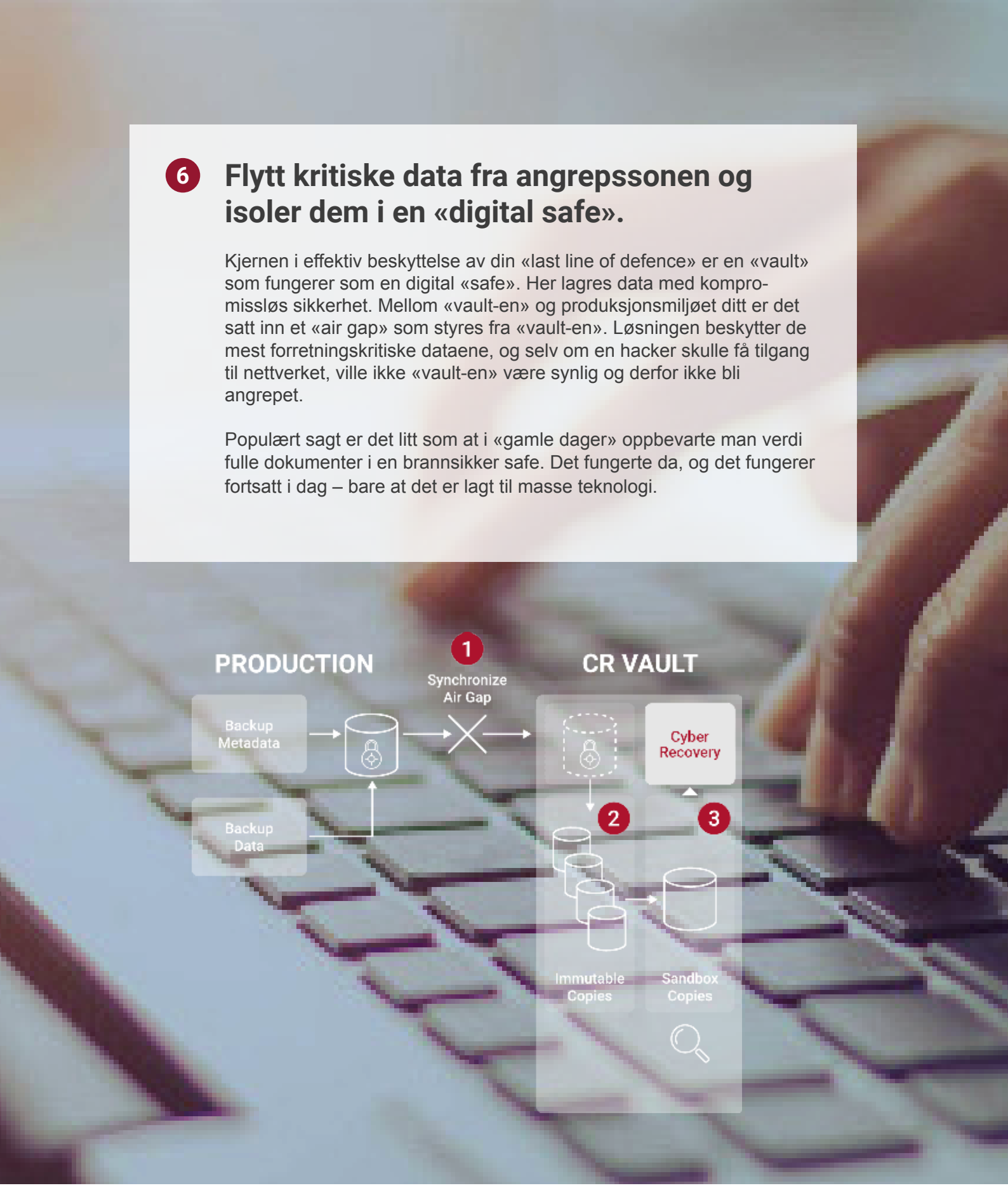
5 Det finnes en løsning der selv dyktige hackere ikke får tilgang til backupen din

Forestill deg at en cyberkriminell vil trenge seg inn i virksomheten din. En av kollegene dine har klikket på noe i en e-post som slapp hackeren inn, og nå er det en ganske fritt fram. Men ikke helt allikevel, fordi hackeren kan ikke se og få tilgang til backup-dataene dine. Saken er at den cyberkriminelle har støtt på noe som effektiv beskytter backupen mot angrep: Dell EMC PowerProtect Cyber Recovery er designet for å automatisere end-to-end-workflows med det formål å beskytte forretningskritiske data, identfisere mistenkelig aktivitet og – om nødvendig – gjenopprette gyldige data.

6 Flytt kritiske data fra angrepssonen og isoler dem i en «digital safe».

Kjernen i effektiv beskyttelse av din «last line of defence» er en «vault» som fungerer som en digital «safe». Her lagres data med kompromissløs sikkerhet. Mellom «vault-en» og produksjonsmiljøet ditt er det satt inn et «air gap» som styres fra «vault-en». Løsningen beskytter de mest forretningskritiske dataene, og selv om en hacker skulle få tilgang til nettverket, ville ikke «vault-en» være synlig og derfor ikke bli angrepet.

Populært sagt er det litt som at i «gamle dager» oppbevarte man verdi fulle dokumenter i en brannsikker safe. Det fungerte da, og det fungerer fortsatt i dag – bare at det er lagt til masse teknologi.



7 Bruk den nyeste teknologien i kampen mot hackerne

Med Cyber Recovery tar du med deg Artificial Intelligence og Machine Learning inn på slagmarken. Dette gjøres i form av løsningens analysemotor, som kjøres på daglig basis inne i «vault-en». Motoren analyserer hendelser basert på kjente cyberangrepsstrukturer, og den sammeligner kontinuerlig dagens skanninger med gårsdagens. Hvis sammenligningen identifiserer store endringer i datastrukturen, vil du motta en alarm. Dermed blir et cyberangrep oppdaget mye tidligere enn vi ofte ser i dag. Reaksjonstiden reduseres fra 3–6 måneder til 24 timer!

8 Velg en løsning som automatisk gjenoppretter data og løser problemet

Hvis du blir utsatt for et angrep i produksjonsmiljøet ditt, kan Cyber Recovery gi deg en rask løsning i form av rene data fra «vault-en», gjenoppretting av kritiske systemer og vende tilbake til normale forhold. Dette gjøres i samarbeid med PowerProtect Data Manager og krever at du kjører Dell EMC NetWorker Cyber Recovery. Effektiv beskyttelse av dataene dine er – som du vet – en ikke helt ukomplisert affære og foregår i et effektivt samspill mellom flere «forsvarssystemer».

9 Lag en overordnet plan for størst mulig digital motstandskraft

I mange år har Dell Technologies utviklet og levert effektive og sikre sikkerhetskopieringsløsninger med sin DataDomain. Cyber Recovery er det sterke forsvaret mot hackernes nye atferd. Når vi snakker digital motstandskraft generelt, vil vi råde deg til å se på helhetsbildet av teknologier og forretningsprosesser i din bedrift, og lage en plan for oppsettet ditt, gjerne i samarbeid med oss i Serit.
Serit noen av de høyest sertifiserte Dell EMC-konsulentene i Norden. Derfor kan du trygt la oss hjelpe med planlegging, rådgivning og implementering.

10 Få en peronlig demo av oss og se hvordan den digitale «safen» beskytter dataene dine

Vil du oppleve hva som skjer når bedriftenes kritiske data lagres «bak lås og slå», slik at cyberkriminelle må gå med uforfettet sak? Og vil du bli introdusert for Artificial Intelligence og Machine Learning i kampen mot cyberangrep?

Kontakt oss for å bestille en personlig demo av Dell EMC Cyber Recovery.

Vi har løsninger som får hackeren ut av backupen din

Kontakt oss og få mer informasjon

Serit gruppen

E-post: post@serit.no
www: serit.no

serit
Smart IT. God jobbdag.