Trinvis guide: Databeskyttelse.

Af Alan Radding

Når it-chefer diskuterer databeskyttelse, er virksomhedens størrelse irrelevant. "Mellemstore virksomheder har det samme behov for at beskytte deres data som store virksomheder, de har blot færre ressourcer til rådighed", siger Mike Karp, chefanalytiker hos Ptak, Noel & Associates. Hvis virksomhedens data kompromitteres eller ikke er tilgængelige, udgør det et stort problem for virksomheden, uanset størrelse. "Det er et spørgsmål om, hvor længe du kan fungere uden at have adgang til dine data", fortsætter han.

Svaret: Kun nogle timer, mener Karp. En dag eller mere uden adgang til virksomhedens data rejser spørgsmål om, hvorvidt virksomheden kan overleve. Virksomheden kan ligeledes gøre sig skyldig i overtrædelse af branchespecifikke lovbestemmelser om beskyttelse af bestemte typer data.

"Databeskyttelse betyder oftest sikkerhedskopiering af data til bånd eller til disk, som er mest udbredt i dag", siger Greg Schulz, senioranalytiker hos StorageIO. Mellemstore virksomheder står dog over for en række udfordringer, når det drejer sig om sikkerhedskopiering af data. Sikkerhedskopiering har tidligere involveret komplicerede processer, som ofte forudsætter særlige IT-færdigheder og er forbundet med ekstra omkostninger. Udbredt servervirtualisering kombineret med lovkrav om beskyttelse af bestemte typer personlige data gør ikke billedet mindre komplekst.

Brancheanalytikere har defineret en standardproces i seks trin til beskyttelse af data. Det er muligvis ikke nødvendigt for mellemstore virksomheder at følge alle seks trin, men det er vigtigt, at de ved, hvad de skal gøre, og hvilke muligheder de har.

Trin 1

Vurder, registrer og klassificer virksomhedens data

Dette er et spørgsmål om at identificere alle data, herunder hvor de er placeret, og hvordan de beskyttes i dag. Virksomhedens ledere skal derefter klassificere dataene efter deres betydning for virksomheden. Nogle data, f.eks. transaktionsdata eller kundedata, er vigtige. Andre data er mindre vigtige.

Undersøg til sidst, om nogle af dataene er underlagt særlige lovbestemmelser. Hvis du gemmer fortrolige personlige oplysninger, f.eks. cpr-numre, kan der være særlige krav til beskyttelse af disse data.

Trin 2

Bestem RPO og RTO

Gendannelsespunkter (RPO) og gendannelsestid (RTO) er nøgleparametre, når det drejer sig om beskyttelse af data. Disse nøgleparametre er uløseligt forbundet med, hvor meget en virksomhed skal investere for at opnå tilstrækkelig databeskyttelse.

- **Gendannelsespunktet (RPO)** er det punkt i fortiden, f.eks. to timer eller to dage, hvorfra du vil gendanne data.
- **Gendannelsestid (RTO)** er den acceptable tid, som det tager at gendanne dine data, hvis du har behov for det.

Du kan bruge følgende generelle tommelfingerregel: Jo tættere på nul, du angiver RPO og RTO, jo mere koster det. Mellemstore virksomheder kan som regel klare sig med en RPO og RTO i timer eller endda en dag. Det betyder, at de kan reducere omkostningerne til databeskyttelse betydeligt, uden at virksomheden løber nogen nævneværdig større risiko. Det er derfor, det er vigtigt, at dataene klassificeres lige fra starten. Ikke alle data har den samme værdi eller behøver den samme RPO og RTO.

Trin 3

Forstå, hvilke muligheder du har for databeskyttelse

Der findes stadigt flere muligheder for databeskyttelse. Brancheanalytikere er generelt enige om tre muligheder, som er velegnede til mellemstore virksomheder. Disse tre muligheder er: Sikkerhedskopiering til bånd, sikkerhedskopiering til disk, ofte med anvendelse af et virtuelt båndbibliotek, samt fjernreplikering.

- **Sikkerhedskopiering** til bånd er den sikre databeskyttelsesløsning til mellemstore virksomheder. Båndløsningen understøttes af softwareværktøjer til sikkerhedskopiering, processen er velkendt, selvom den er en smule tung og langsom, og det er muligt at lagre bånd eksternt for at øge beskyttelsen yderligere.
- **Sikkerhedskopiering** til disk: Adgangen til økonomiske diskdrev gør det muligt at sikkerhedskopiere data til disk. Diske understøtter hurtigere og mere pålidelig sikkerhedskopiering og gendannelse af data. Virksomheder flytter ofte de sikkerhedskopierede data til bånd efter en bestemt periode, typisk på mellem en uge og en måned, for at frigøre diskplads til flere sikkerhedskopier. Virtuelle båndbiblioteker får disken til at fremstå som et bånd for sikkerhedskopieringssoftwaren, så virksomheden slipper for at ændre sikkerhedskopieringsproces.
- **Fjernreplikering** sender kopier af de lagrede data over netværket til et eksternt sted, hvor de kan lagres på disk eller bånd. Dette giver ekstra beskyttelse.

"Du kan betragte fjernreplikering som et værn imod ulykke", siger Karp. Flytning af bånd til et eksternt sted udgør et ekstra beskyttelsesværn.

Trin 4

Vælg den rette kombination af muligheder

"Der findes ingen enkelt mulighed, som passer til alle mellemstore virksomheder, og mange virksomheder anvender en kombination af flere muligheder", siger Schulz. Du kan f.eks. anvende sikkerhedskopiering til disk eller virtuelle båndbiblioteker til data, hvor der er behov for en lav RPO og RTO, og sikkerhedskopiering til bånd til data, som du kun sjældent har brug for. Det drejer sig om at vurdere, hvor vigtige dataene er for virksomheden, og forstå den nødvendige afvejning mellem RPO og RTO.

Virksomheder replikerer i nogle tilfælde data til satellitkontorer af sikkerhedsmæssige hensyn, men det er en god ide at oprette en sikkerhedskopi af dataene forud for replikeringen. "Satellitkontorer råder kun meget sjældent over ressourcer til beskyttelse af data", siger Karp. Hvis det blot er et spørgsmål om at flytte dataene væk fra virksomheden, kan du også sende bånd til fjernkontoret med henblik på opbevaring.

Trin 5

Håndter virtualiseringsudfordringen

Udbredelsen af virtuelle servere gør databeskyttelse endnu mere kompleks. "I et virtuelt servermiljø er det særligt vigtigt at have en solid databeskyttelsesstrategi", siger Schulz. Desværre mangler flere af de aktuelle virtualiseringsprodukter på markedet værktøjer til komplet databeskyttelse, fortsætter han.

De grundlæggende værktøjer til virtuel sikkerhedskopiering understøtter sikkerhedskopiering af hele den virtuelle maskine. Det er først muligt at gendanne data, når hele den virtuelle maskine er blevet genoprettet. Virksomheder ønsker dog typisk ikke at genoprette alt, men blot en enkelt fil eller to. Der findes leverandører, som tilbyder proxyprodukter, der opfylder dette behov.

Trin 6

Kryptering og overholdelse af lovkrav

Virksomheden kan være underlagt branchespecifikke lovkrav om at beskytte bestemte personlige data gennem anvendelse af kryptering. Dette gælder særligt for data, som sendes over et netværk.

Mange lande har en lovgivning, som kræver, at personlige data skal krypteres, så de er beskyttet i tilfælde af databrud. Ellers er virksomheden i tilfælde af datatab forpligtet til at underrette de personer, hvis data er blevet kompromitteret. Mange virksomheder vælger at kryptere lagrede private data.

Mellemstore virksomheder kan vælge mellem adskillige databeskyttelsesmuligheder til særdeles attraktive priser. Leverandørerne har endvidere tilført produkterne intelligens for at forenkle processen. Med markedets moderne brugervenlige, økonomiske løsninger til sikkerhedskopiering til disk, er der ikke nogen grund til ikke at beskytte sine data.

Alan Radding er bosiddende i Newton, Massachusetts, og har stor erfaring som freelanceanalytiker og forfatter med speciale i virksomheder og IT.