

POWERED BY:

COMPUTERWORLD

Artiklerne er skrevet af Lars Danielsson, ComputerSweden

WHITEPAPER

Datasikkerhed

**Information er ofte det eneste, din virksomhed har.
Sørg for at beskytte den**

SPONSORERET AF:



INDHOLD

1. PROBLEMET. Uden data dør virksomheden. Løsningen er at fokusere på nogle enkelte problemområder	2
2. TRUSLEN. Mange vil forsøge at få adgang til dine hemmelige data. Følg syvpunkts-listen for at forhindre, at truslen rammer dig	5
3. MOBILITET. Mobile data gør det sværere – udfordringen er at vide, hvor alle data befinder sig	8
4. LIVLINEN. Sådan fungerer kopiering i dag – og så sådan sørger du for, at kopierne også er til at stole på, når uheldet rammer	10
5. Opgaver. Find de rigtige definitioner og lær dig de vigtigste måder at sikre kvaliteten på dine almindelige data	13
6. BESKYTTELSE Her er de forskellige softwaretyper som beskytter dig – men du skal ikke stole blindt på dem	16

1. Uden data dør virksomheden

Mister du dine data, dør din virksomhed. Så galt kan det gå. Løsningen er at arbejde med forskellige områder, så du kan skabe en bedre beskyttelse af din virksomhed.

Søger du på ordene datatab og nedbrud, er der stor chance for, at du finder en webside med følgende tekst:

"Vores serverleverandør har haft indbrud i sine servere, hvilket førte til totalt datatab samt stort nedbrud blandt deres servere". At siden så ikke har været opdateret i over et år taler sit tydelige sprog.

Sløseri med datasikkerhed kan føre til store problemer og i værste fald til konkurs. Der er ikke tale om skræmmekampagner eller luskede markedsføringstrick fra en sikkerhedsvirksomhed. Det er sandheden.

I en artikel fra oktober omtaler Computerworlds søsterblad CIO en undersøgelse udført af Tele2, som viser, at "hvert fjerde mindre virksomhed tager ikke backup".

Hvordan hænger det så sammen? Det gør det heller ikke. Er det et potentielt problem, så burde man anstrenge sig for at forebygge det. Eller hvad?

Men datasikkerhed er ikke alene besværligt og dyrt. Det er også et uhyre bredt område.

Eller rettere, det er flere områder med samme fællesnævner; nemlig at man risikerer ikke at kunne anvende data på den rigtige facon, enten fordi man taber data, eller fordi data ikke er korrekte. Samtidig er der en risiko for, at følsomme data handler i de forkerte hænder.

Flere aspekter

I dette kompendium ser vi på flere aspekter af datasikkerhed: Sikkerhedskopiering, indbrud og skadelig kode, sikkerhedsprogrammer, mobilitet og datakvalitet.

Det handler kort og godt om at beskytte sig mod, at data forsvinder af tekniske årsager og at vide, hvilke trusler der findes fra fjendtlige personer, og hvordan man kan beskytte sig – mod dem.

Det gælder om at gøre data tilgængelige for ansatte i virksomheden, der hvor personerne er, på en sikker måde. Og endelig handler det om at sikre, at data – som man arbejder så hårdt på at beskytte – er brugbare.

Tænk lidt over, hvilke data eller hvilken database, der er vigtigst for din virksomhed. Tænk på, hvad konsekvenserne ville være, hvis data forsvandt og ikke kunne genskabes. En dag uden salg? Rigtigt vrede kunder? Stop i produktionen? Måske konkurs?

Prøv at regne på, hvad en sådan ulykke kunne koste. Det beløb kunne man godt satse på datasikkerhed. Nu.

To standarder

Ifølge organisationen Open Security Architecture der to ansete internationale standarder, som handler om it-sikkerhed: ISO 27001 og Nist 800.

Begge handler primært om fortrolighed, integritet og tilgængelighed. Desuden tages områder som ægthed og sporbarhed op.

Information koster

Få har gjort det, men når der gøres forsøg på at vurdere data, viser det sig, at data i sig selv kan være uhyre værdifulde.

Selvfølgelig er data værdifulde, Men præcis hvor værdifulde er de? Sikkerhedsvirksomheden Symantec har forsøgt sig med envurdering i forbindelse med, at to statsansatte i Storbritannien forliste to cd'er med information om 25 millioner britiske borgere. Cd'erne indeholdt oplysninger om adresse, forsikringer og i visse tilfælde også bankoplysninger. Ifølge Symantec ville informationerne kunne sælges for 100 dollars pr. person på det sorte marked. En virksomhed kan naturligvis ikke vurdere sine egne data efter de priser, der er gældende blandt kriminelle. Men i flere lande arbejdes med at forsøge at vurdere datalagre, store databaser med informationer til beslutningsstøtte, for at kunne medtage værdien i bogføringen.

Værdifulde data

Den australske virksomhed Spatial Information Systems publicerede i marts en rapport om værdien af geografiske data i Australien. Konklusionen er, at geografiske data bidrager med mellem 25,7 og 50,4 milliarder kroner til det australske bruttonationalprodukt. Det svarer til mellem 0,6 procent og 1,2 procent af det samlede bruttonationalprodukt.

En af grundene til, at tallet er så højt, er at de geografiske data bidrager til at øge husholdningernes forbrug med mellem 14,3 og 27,4 milliarder kroner, fremgår det af undersøgelsen.

Desuden bidrager de til at øge investeringerne med mellem 6,9 og 14,7 milliarder kroner pr. år, og samtidig bliver eksporten, ifølge Spatial Information Systems, op til 9,2 milliarder kroner højere.

Sunde sikkerhedsstrategier

I samme sekund, man beslutter at investere, skal man iværksætte initiativer for at sikre og beskytte data. Det lønner sig i længden.

Ikke nok med at det er kedeligt at købe ind, installere, konfigurere og installere programmer på servere, klient-computere og mobiler. I alle stadier skal man også tage hensyn til sikkerhedskopiering, databeskyttelse og -kvalitet.

Og når driften er kommet i gang, gælder det om at kontrollere, at alt fungerer, som det skal.

Hvis vi ser på sikkerhedskopiering til at begynde med, er det så virkelig nødvendigt? Hvor ofte går den server, hvor virksomhedens vigtigste database ligger på, ned? Kan det ikke bedre betale sig at tage bøvlet, når det sker, hvilket statistisk set ikke burde være så ofte?

"Man kan ikke med sikkerhed regne ud, at det skulle være billigere at undlade at sikkerhedskopiere," siger Åke Ljungvist, chef for Ibas i Sverige.

Ibas beskæftiger sig med at redde, fjerne og efterforske data.

"Forebyggende sikkerhedsforanstaltninger betaler sig altid i længden".

Det vigtigste, når vi taler sikkerhedskopiering, er at sørge for, at alle brugere lagrer data i netværket og ikke lokalt på deres egne computere. På den måde bliver det enklere og billigere at foretage sikkerhedskopiering.

Sikkerhed som rutine

Så vidt så godt. Men hvor alvorligt skal man tage indbrudsforsøg og andre trusler som f.eks. vira? Er der en reel risiko for, at virksomhedens data bliver stjålet eller ødelagt?

"I samme øjeblik en virksomhed kobler sig på internet, er den eksponeret. Uanset virksomhedens størrelse vil der være en konstant trafik, som observerer, hvad der foregår," siger Predrag Mitrovic, chef for Labcenter i Sverige.



Hvor farligt er det?

"Virksomheder, hvor et aktivt sikkerhedsarbejde ikke er en del af rutinerne, kan godt regne med, at der vil være indbrudsforsøg. Budskabet er tydeligt: Hvis du ikke arbejder med at beskytte dine data, så går det galt".

Datakvalitet

Det, der gælder for almindelige computere med hensyn til sikkerhedskopiering og beskyttelse mod ulovlig indtrængning, gælder også for avancerede mobiltelefoner, de såkaldt smart phones.

Men at dømme efter de sikkerhedseksperters, Computerworld har talt med, er teknikken mindre udviklet til telefonerne. Og desuden sløses der ofte med brugen af de løsninger, som findes. Sidst, men ikke mindst, gælder det datakvalitet. Der er ingen ide i at kopiere og beskytte data, hvis der er fejl på dem.

"Dårlig datakvalitet fører til lange diskussioner om, hvordan virkeligheden ser ud, i stedet for at kunne basere sig på fakta," siger Hellen Wohlin Lidgard, direktør for konsulentvirksomheden Pointer Sweden.

Og netop datakvalitet er måske det sværeste område, vi tager op her i kompendiet.

For at det kan lykkes, skal man starte fra bunden. Begynde med at definere de begrebet, som anvendes i en virksomhed som eksempelvis, hvad en "kunde" er rent definitionsmæssigt.

Pas på internettet

Ifølge Gartner og Symantec sker omkring 75 procent af data-indbrudsforsøg via webapplikationer.

Ifølge Microsoft er 64 procent af webudviklerne ikke sikre på, at de kan skrive sikre applikationer.

Aberdeen Group rapporterer, at 70 procent af udviklingsfirmaerne ikke har sikkerhedstankegang indbygget i udviklingsprocessen.

Gartner regner med, at 80 procent af alle virksomheder vil have været udsat for angreb før 2010.

Kilde: IBM

2. Trusselsbilledet 2009

Antallet af indbrudsforsøg på internet kan med sikkerhed opgøres i millioner. En enkelt bruger kan være udsat titusindvis af gange i døgnet.

Alle, der er tilsluttet internet, løber en risiko for at blive udsat for indbrudsforsøg. Det gælder ikke mindst virksomheder. Det betyder, at nogen forsøger at få kontrol over brugernes computere, eksempelvis for at lede efter følsomme informationer, installere programmer med skadelig kode, sende skadelig kode videre eller bare ødelægge.

Der er tale om en reel trussel mod virksomhedsdata.

”En computer, som er tilsluttet Internet, bliver udsat for indbrudsforsøg konstant, flere gange i minuttet,” siger Oskar Bergqvist, it-sikkerhedstekniker på Sitic, (Sveriges it-incident centrum).

Sitic er en del af den svenske post- og telestyrelse og dermed en statslig organisation, der har til formål at hjælpe virksomheder og myndigheder med it-sikkerhed.

Ifølge Oskar Bergqvist er de fleste indbrudsforsøg automatiske scanninger, der leder efter sårbare systemer. Sitic har værktøjer, der kan finde og registrere skadelig kode og indbrudsforsøg:

”Om et indbrudsforsøg er alvorligt afhænger helt af, hvad din virksomhed klassificerer som alvorligt. De automatiske scanninger er relativt lette at beskytte sig mod”, siger han.

Måltrettede angreb

Det er svært at opdage mere avancerede angreb, som forsøger at gemme sig i mængden.

”De alvorlige indbrudsforsøg holder ofte en lavere profil og strækker sig ikke sjældent over en længere tidsperiode,” siger Oskar Bergqvist.

Ifølge Thomas Nilsson, grundlægger og medejer af it-sikkerhedsvirksomheden Certezza er det netop de måltrettede indbrudsforsøg, man skal holde øje med.

”De udgør ganske vist kun en lille brøkdel af den samlede mængde, men forskellen er, at man ofte udnytter brister hos den enkelte bruger”.

Risikoen for at blive ramt af et måltrettet indbrudsforsøg er koblet til, hvad virksomheden beskæftiger sig med. Jo flere penge, eller jo mere følsomme informationer, det håndteres, jo flere indbrudsforsøg vil virksomheden blive udsat for.

Sitic informerer om aktuelle trusler. Et eksempel er fra april 2008, da man rapporterede, at flere svenske hjemmesider var inficerede med kode, som sendte brugeren videre til websider, hvor der skete et forsøg på at installere skadelig kode på brugernes computere.

En af de ramte fortæller, at han blev udsat for indbrudsforsøg mellem hver tredje og hver sjette sekund – alene på Microsofts chattjeneste Windows Live Messenger.

Det betyder mindst 14.400 indbrudsforsøg i døgnet alene for en bruger og et websted.

Så at en virksomhed bliver udsat for hundredtusindvis af indbrudsforsøg i døgnet er ikke en urimelig tanke.

Howdan får kriminelle organisationer oplysninger om, hvor det kan betale sig at forsøge sig med indbrud?

”Nøjagtig som med en søgemotor sker der en konstant kortlægning af systemer, som er sluttet til internet,” siger Predrag Mitrovic fra Labcenter.

Usikker vurdering

Et eksempel på, hvor svært det kan være at vurdere omfanget af spredning af skadelig kode, er Sitics rapport om virussen Storm Worm, som blev spredt til mange brugere forrige år via mail og websteder.

Antallet af computere, der blev inficeret, skønnes at være mellem 160.000 og 50 millioner. Det eneste, man kan konstatere med sikkerhed, er, at mange computere blev inficeret.

Før det går galt

Brug det rigtige program til at beskytte dig og koncentrer dig om de alvorlige trusler. Her er syv vigtige punkter.

1 Konfigurer systemerne
Der bør være en fast rutine til at danne sig et overblik over alle konfigurationer, eksempelvis applikationer og operativsystemer. Der findes informationstjenester, som viser, hvilken angrebstrafik, der for tiden er mest udbredt. Ved hjælp af den information kan man kontrollere konfigurationerne.
"Normalt gælder det om at konfigurere systemerne rigtigt og holde dem opdaterede. Det er et arbejde, der aldrig bliver færdigt", siger Per Hellqvist, specialist i it-sikkerhed i Symantec.

2 Luk for tjenester
Det er vigtigt at gøre målet mindre, for eksempel ved at lukke for tjenester, som reelt ikke bliver brugt. Hvis man så får brug for en tjeneste eller applikation, kan man åbne den for visse brugere og lægge speciel overvågning på den, anbefaler Per Hellqvist.

3 Begræns antallet af rettighedsmodeller
Ved at gøre antallet af rettighedsmodeller mindre bliver det enklere at holde styr på dem. Ifølge Predrag Mitrovic fra Labcenter er det vigtigt at kontrollere, at sikkerhedsopdateringer ikke åbner noget, der ikke skulle være åbent.

4 Brug firewalls
Det er nødvendigt med firewalls. Der findes også applikationer som giver et ekstra lag af beskyttelse mod indbrud, de såkaldte intrusion detection-systemer

5 Koncentrer dig om de alvorlige trusler
For hver million rækker i en log er der måske tusind interessante, og af dem er måske 2-5 så alvorlige, at man bør se nærmere på dem.

6 Sørg for beskyttelse på flere niveauer
Thomas Nilsson fra it-virksomheden Certezza fremhæver, at det er vigtigt at anvende både lokalt installerede sikkerhedsprogrammer og webtjenester. Det gælder om at have beskyttelse på alle niveauer både fysisk i form af hardware og i de applikationer som kører.

7 Hold styr på menneskene
Sikkerhed handler ikke kun om programmer. Det er en urealistisk tiltro til, hvad man kan klare med teknik. "Det svage led i den sammenhæng er brugeren," siger Thomas Nilsson fra Certezza.

Applications

“Unlimited”

Oracle – Siebel – PeopleSoft – JD Edwards

- ✓ **Continued New Releases**
- ✓ **Customer Driven Product Roadmaps**
- ✓ **Dedicated Development Teams**
- ✓ **No Forced Migrations**

Get better results with proven applications tailored for your industry, processes and geography.

ORACLE®

oracle.com
or call 1.800.ORACLE.1

3. Mobil information gør beskyttelse sværere

Virksomheder lægger ikke lige så meget arbejde i at sikre mobile løsninger som på at sikre traditionel it. Det største problem er at holde styr på, hvor data befinder sig.

Mobilitet har længe været en stærk tendens inden for it, og der er absolut ingenting, der tyder på, at den trend skulle mindske i styrke. Det medfører problemer for datasikkerheden. "I dag findes der formentlig ingen it-sikkerhedschefer, som har styr på, hvor al information i virksomheden findes," siger Per Hellqvist, specialist i it-sikkerhed i Symantec. Han mener, at det må være anstrengende, når informationer, som man skal beskytte, er spredt vidt omkring.

Hvordan skal man angribe problemet?

"Arbejder man ud fra, hvem der skal have hvilken information på hvilken enhed, kan man klare de fleste udfordringer," mener Per Hellqvist.

Tre spørgsmål

Det handler altså om at besvare tre spørgsmål for at sikre datasikkerheden i mobile miljøer.

"Hvem" gælder, om en person behøver være mobil eller ikke samt, hvilken information personen skal have adgang til baseret på personens rolle i virksomheden.

"Hvilken information" gælder, hvordan informationen er klassificeret, om den er intern, følsom, hemmelig eller åben. Eksempler på forskellige typer af information er kunderegister, ordrebekræftelser, intern telefonoversigt, egne mails og dokumenter.

"Hvilken enhed" gælder, om enheden er tjekket og godkendt af it-afdelingen.

Det indebærer, at man har undersøgt, hvordan enheden kan beskyttes og understøttes, eksempelvis med antivirusprogrammer, firewall, kryptering, patch-håndtering samt konfigurationshåndtering.

Eksempler på enheder er forskellige typer avancerede mobiletelefoner, men det kan i princippet også handle om bærbare computere.

Ringe mobil beskyttelse

Spørgsmålet er, hvor mange virksomheder, der reelt arbejder ambitiøst med mobil datasikkerhed.

"Mange gange er det overraskende, hvordan man tænker i de her sammenhænge," siger Thomas Nilsson, grundlægger og medejer af it-sikkerhedsvirksomheden Certezza.

Han fortæller, at der er en tendens til, at virksomheder ikke arbejder på samme måde med sikkerheden, når det gælder mobile løsninger.

Som regel vurderer man, hvordan kommunikationen skal sikres, hvordan informationen skal lagres, og hvordan rettigheder skal ordnes, inden man går i gang med en højrisiko-ordning.

"Men når det gælder mobilen, er mange fascinerede over, at man kan synkronisere mail, kalender, kontakter og databaser, men glemmer det, som i alle andre sammenhænge er indlysende," siger han.

Desværre er mange af de tidlige mobile projekter gjort permanente, med alle de risici det indebærer.

"Det er den barske og ildevarslende sandhed," siger Thomas Nilsson.

Og problemet er almindeligt. I en nogenlunde it-moden organisation er det efterhånden snarere reglen end undtagelsen at anvende mobiletelefoner til mere end bare ringe, fortæller Tomas Nilsson.

Og der er en grund til det.

"Der er enorme fordele ved at lade medarbejderne arbejde, hvor og når de vil. Har man bare styr på, hvilke informationer der befinder sig hvor, kan man tillade meget mere," siger Per Hellqvist.

Mobilitet øger effektiviteten, men kun hvis det bruges på en sikker måde.

Mobiltelefonen – en andenrangs medborger

Det kan være svært at administrere mobiltelefoner, til trods for at de i bund og grund fungerer som en computer.

En mobiltelefon og en computer er på mange områder ligeværdige. Der er operativsystem, filsystem, grafisk brugerflade og applikationer i begge dele.

Hvorfor er det sværere at håndtere sikkerheden i mobiltelefoner?

”Det er en udfordring at få mobiltelefoner ind i bruger- og enhedsbibliotekerne og at styre distributionen af programmer,” siger Predrag Mitrovic, chef for Labcenter i Stockholm.

En anden forskel er, at rettighederne delvis styres af teleoperatøren. Der er altså en ekstra faktor at tage hensyn til.

Det er også mere teknisk betingede sikkerhedsproblemer med mobiltelefoner.

”Mobilens kapacitet er begrænset. Klassisk beskyttelse æder mere eller mindre hele kapaciteten, og i bedste fald kun batterierne, siger Thomas Nilsson grundlægger og medejer af it-sikkerhedsvirksomheden Certezza.

Det er formentlig en af grundene til, at sikkerhedsprogrammer ikke anvendes i samme udstrækning på mobiltelefoner som på computere.

”Der findes krypteringsløsninger, men de anvendes ikke meget. Jeg kan ikke forstå hvorfor, eftersom der ikke findes mange ting, der stjæles lige så meget som mobiler. Det samme gælder bærbare computere, siger Per Hellqvist fra Symantec.

Og har man ikke beskyttet informationerne på en mobil, kan de let havne i de forkerte hænder.

”Husk også at kryptere hukommelseskortene”, siger han.

Webtjenester er risikable

Mobilitet handler ikke kun om mobiltelefoner, men også om bærbare pc'er. De bruges også med sikre tilslutninger, såkaldt VPN, virtuelle private net.

Men er et VPN via internet lige så sikkert som at sidde på kontoret og arbejde i det lokale netværk?

”Nja – der findes parametre, som er svære at håndtere. Det lægges desværre for lidt arbejde i det her, man bøjer sig for brugernes krav, mener Per Hellqvist.

Yderligere et aspekt ved mobilitet er brugen af webtjenester i stedet for traditionelle programmer. Webtjenesterne indebærer, at en bruger kan få adgang til data hvor som helst fra - i princippet - en hvilken som helst computer.

”Webtjenesterne udgør en risiko i alle sammenhænge, hvor informationerne ikke kontrolleres af en egen virksomhed. Alt for ofte fraskriver leverandørerne sig ansvar ved en eventuel skade,” siger Per Hellqvist.

Mangler virusbeskyttelse

Mobiltelefonbrugere er ligeglade med virusbeskyttelse, og brugen af webtjenester stiger.

Brugen af sikkerhedsprogrammer er ikke så almindelig på avancerede mobiltelefoner, de såkaldte smart phones. Det er dem, der fungerer som klienter i virksomhedsløsninger.

Nokia dominerer

Salget af smart phones i Europa, Mellemøsten og Afrika i tredje kvartal 2008 i millioner.

Nokia 9,2

Apple 1,4

HTC 1,1

Andre 1,8

Kilde: Gartner

4. Sådan fungerer kopiering i det nye århundrede

Sikkerhedskopiering sker ikke i dag som i fars tid. Nu er det lagring på disk, replikering og cloud-tjenester, det gælder.

Alle ved, at man skal sikkerhedskopiere, men alligevel sløser mange. Det er svært at sørge for, at rutinerne for sikkerhedskopiering følger med it-udviklingen.

”Når mængden af information typisk vokser med 50-60 procent pr. år bliver håndteringen af sikkerhedskopier en stor udfordring” siger Max Leissner, produktchef i EMC.

Trods nye teknikker og løsninger fortsætter mange virksomheder med traditionel backup til traditionelle medier. I praksis betyder det, at de kopierer data til bånd.

”Det gøres primært for at vær sikker på, at der er kopier ”et andet sted””, siger Max Leissner.

Men stadig flere virksomheder, primært de større, retter blikket mod nye løsninger. Det skyldes først og fremmest, at der er behov for nye tiltag i distribuerede miljøer, altså flere geografisk spredte kontorer og i hårdt konsoliderede miljøer eksempelvis når der anvendes virtualisering.

Max Leissner taler om ”global deduplicering” og ”geografisk replikering af filsystemer”. I klartekst betyder det, at man sender data rundt til forskellige diske på forskellige steder, så de er tilgængelige flere steder. Så hvis et data-center brænder op, kan data findes intakte et andet sted.

Syntetisk backup

Åke Ljungqvist, som er sverigechef i dataredningsfirmaet Ibas udtrykker det på denne måde:

”En trend er at kopiere til disk ved korttidslagring, så man hurtigt får adgang til data. Kopiering til bånd gælder ved langtidslagring.

En anden tendens er, at ikke mindst de små virksomheder satser på tjenester på web i stedet for selv at have udstyret til sikkerhedskopiering. De kopierer informationer til en server på internet, altså backup i skyen.

”Det er et af de områder, hvor cloud computing-tjenester er mest konkrete,” siger Max Leissner.

Et af de største problemer med sikkerhedskopiering er, at datamængderne er så store.

”En måde at løse problemet på er at foretage såkaldt syntetisk backup, hvor man kun tager backup af ændrede data”, siger Jonas Alstermark, der er områdechef for server og storage i HP i Sverige.

Uanset hvor teknisk avancerede løsninger, man har, er det svært at garantere, at alle data kopieres.

”Et stort problem er, at mange lægger ansvaret for sikkerhedskopieringer på brugeren, siger Åke Ljungqvist.

Problemet er bare, at brugeren tror, at it-afdelingen gør, hvad der skal gøres for at beskytte data. Men hvis data bliver lagret et ”forkert” sted, for eksempel lokalt på en klient-pc, bliver de ofte slet ikke kopieret.

”Her tegner de bærbare pc’er sig for en stor del af problematikken,” siger Åke Ljungqvist.

Har du nu også kopieret filerne?

En rutine for backup er ikke komplet, før man har kontrolleret, at alle kopierne også kan bruges.

Lad os sige, at din virksomhed har gjort et forbilledligt arbejde med at skabe rutiner for sikkerhedskopiering. I har undersøgt, hvilke data der bør kopieres, og hvordan de skal kopieres. Og I har også kørt backuppen.

Så kommer dagen, da katastrofen indtræffer. "Intet problem", tænker alle, "vi har jo kopier".

Men da kopierne skal indlæses, er der båndene tomme. Nogen har glemt at kontrollere, at kopierne kunne bruges. "Det sker oftere, end man tror, at data som sikkerhedskopieres ikke kan læses ind," siger Max Leissner fra EMC. Tidligere var den hyppigste årsag til sådanne problemer, at der var bøvl med backupmedierne.

"Vi støder stadig oftere på administrationsfejl. Man tror, at sikkerhedskopieringen er god nok, men når informationerne skal genindlæses, viser det sig, at der mangler vigtige informationer. Man tester backuppen, og når det virker, som om den kører godt, så stiller man sig tilfreds med det," siger Max Leissner.

Rutiner mangler

Åke Ljungqvist fra Ibas oplever, at det er helt almindeligt, at virksomheder ikke har rutiner for at genindlæse og tjekke at backuppen virker.

"Man sætter sin lid til, at backupsystemerne gør, det de skal, og at alt ordner sig, hvis uheldet skulle indtræffe," siger Åke Ljungqvist.

Han påpeger dog også, at det er meget usædvanligt, at data, som sikkerhedskopieres, ikke – i sidste ende – kan genindlæses. I Ibas arbejder man desuden med at redde data fra nedbrudte harddiske.

Så længe mangnetlaget på skiverne i disken ikke er skrabet af eller informationerne overskrevet, er der ifølge Åke Ljungqvist mulighed for at redde data.

Der findes der mange anbefalede metoder for, hvordan sikkerhedskopiering skal ske. Hvilken metode, man vælger, afhænger af flere ting, såsom krav til tilgængelighed til data, datamængder og omkostninger.

"Start med at spørge: Hvor hurtigt skal vi have adgang til sikkerhedskopierne, og hvad må det koste," siger Åke Ljungqvist.

Tænk på miljøet

Det fysiske miljø er vigtigt. Ifølge Åke Ljungqvist, Ibas, er det vigtigt at have lokaler med den rette temperatur og miljø til it-udstyr. Det er ikke usædvanligt, at data går tabt på grund af for høj varme eller dårlig beskyttelse mod ustabilitet i elnettet. Hav kontrol over, hvilke personer, der har adgang til serverrum og lignende lokaler.

Virksomheden bør have en katastrofeplan. Den bør eksempelvis indeholde informationer om, hvem der skal gøre hvad, hvis en katastrofe indtræffer.

Oracle Database 11g

- ✓ Online upgrades and patching
- ✓ Advanced partitioning and compression
- ✓ Record and replay real workloads
- ✓ Delegate jobs to a standby database
- ✓ Query a database as it was a week ago

The Innovation Continues

ORACLE®

**oracle.com/database
or call +353 1 8031099**

5. Dårlig datakvalitet giver unødigt arbejde

Glem ikke at klassificere dine data. Ellers bliver konsekvensen unødige diskussioner og i værste fald fejlagtige analyser. Løsningen er at definere de begreber, der anvendes.

Dårlig kvalitet af data er årsag til mange bekymringer. Her gælder også det gamle ord om "skidt ind – skidt ud".

Hvis data i databaser ikke er komplette eller oven i købet fejlagtige bliver de analyser, der foretages i beregninger til beslutningsstøtte ikke korrekte. Så enkelt er det.

At sikre datakvalitet er et omfattende arbejde, så omfattende at man burde være begyndt med det tilbage i 60'erne eller 70'erne, da de administrative it-systemer gjorde deres indtog i større omfang. Men nu er det ofte for sent at rette de fejl, man begik dengang, og vi må leve med de dårlige beslutninger, der blev truffet i it-æraens barndom.

"Dårlig datakvalitet giver lange diskussioner om, hvordan virkeligheden ser ud, i stedet for beslutninger baseret på fakta, siger Hellen Wohlin Lidgard, direktør for konsulentvirksomheden Pointer Sweden.

Som et eksempel nævner hun en ledelsesgruppe, der diskuterede, hvad rabatter er, til trods for at de udgør et lille bitte tal set ud fra et helhedsperspektiv.

"Hvis der findes definitioner, stopper de her unødvendige diskussioner", siger Hellen Wohlin Lidgard.

Forskellige definitioner

Et af problemerne med præcis beslutningsstøtte er, at informationerne sammenføres fra flere områder. Det er ikke sikkert, at strukturen for data og betydningen af forskellige begreber er ens.

Hvad er det sværeste i arbejdet med at sikre datakvalitet?

"Det svære er at finde og blive enig om, hvad der er det rigtige," siger Hellen Wohlin Lidgard.

Som eksempel på problemer nævner hun, at der i de fleste virksomheder ikke findes et entydigt svar på, hvad en "kunde" er.

Hvordan skal man løse det problem?

"Første skridt er at udpege dataejere blandt virksomhedspersonerne og få dem til at afgøre definitionerne for eksempelvis kunder, produkter og nøgletal.

Hellen Wohlin Lidgard mener, at datakvalitet fortrinsvis er et organisations- og processpørgsmål, ikke et teknisk.

"Har man dataejere og definitioner på plads, kan man skabe enkle værktøjer for datakvalitet. Det gælder om at foretage løbende forbedringer af grundsystemerne".

Mange af de data, som figurerer i beslutningsstøtte kommer oprindeligt fra databaser, ikke mindst relationsdatabaser. Men der findes sikkert endnu flere data i mindre struktureret form som ordrebehandlingsdokumenter og overslag, som ville kunne bruges, hvis man kunne sikre dem.

Så vidt beslutningsstøtte, men hvordan ser det ud med transaktionsintensiv anvendelse?

"Transaktioner holder ofte god kvalitet, problemet skal snarere findes i anvendelsen til beslutningsstøtte," mener Hellen Wohlin Lidgard.

Men det er naturligvis en endnu større katastrofe, hvis transaktionssystemerne, for eksempel til ordrer, har en ringe datakvalitet. Eller endnu værre, hvis der er fejl i bogføringen.

I den moderne it-verden bliver tjenester på web stadig mere almindelig. Spørgsmålet er så, om det bliver sværere at arbejde med datakvalitet med den type tjenester.

Det, mener Hellen Wohlin Lidgard ikke, det behøver blive, men hun påpeger, at det er vigtigt at tage hensyn til tjenesterne, når man skaber processer for kvalitetsarbejde.

En særlig disciplin

Arbejdet med at bestemme, hvad begreber betyder, kaldes ofte for begrebsmodellering. En måde at arbejde med det kan være at oprette arbejdsgrupper med deltagere fra forskellige afdelinger i en virksomhed og sætte sig ned og gennemgå alle vigtige begreber.

Der findes rigeligt med skrækhistorier om hundredvis af definitioner på for eksempel "kunde" i en virksomhed. En sådan begrebsforvirring giver enorme problemer, når man anvender beslutningsstøtte.

De vigtigste udfordringer

Rensning, konvertering og kontrol af data. Der skal mange operationer til for at sikre datakvalitet. Her der de tre vigtigste.

1 ETL. Første skridt, specielt i anvendelse til beslutningsstøtte, er at hente data fra originalkilderne og overføre dem til den ønskede destination, eksempelvis til et datalager, altså en database som er specielt beregnet til beslutningsstøtte. Det arbejde indebærer ofte, at data skal konverteres eller transformeres, om man vil.

På engelsk kaldes dette arbejde ETL, hvilket står for "extract, transform, load". Det er ofte en kompleks proces, som kræver nøje analyse af, hvilke data der er behov for, hvad de egentlig repræsenterer, hvor de findes, og hvordan de skal hentes.

Det er ikke sikkert, at to kundebaser, som skal samkøres, reelt kan køres sammen korrekt. Man kan tænke sig, at datterselskaber behandles forskelligt.

I den ene database lagres hver juridisk enhed måske for sig, mens hele koncerner lagres som en enhed i en anden. Så må man bestemme sig for enten at lægge datterselskaberne sammen i den ene database eller dele dem op i den anden.

Den type arbejde er en del af transformationsfasen, ud over de rent tekniske konverteringer, som at ændre data fra Oracles databaseformat til Microsofts.

Andre udfordringer kan være rent skemamæssige, så som at man kun kan overføre data fra en kilde mellem klokken to og tre om natten.

En sådan begrænsning kan skyldes driftskav for originaldatabasen og sikkerhedsregler.

2 Rensning af data. At rense data eller "data cleansing" er en opgave, som kan udføres før ETL-fasen, under den eller efter den. Det handler om at rette eller fjerne ukorrekte og defekte data.

I visse tilfælde er det let at rense data. Hvis kolonnen til produkt-id er tom i en række i en produkttabel, eller hvis der findes bogstaver i en tal-kolonne, så ved man, at det er en fejl.

I andre tilfælde er det sværere, fordi kontrollerne afhænger af andre data, en dem der kontrolleres.

I det tilfælde må man være sikker på, at kontrol-databasen er korrekt, hvilket så kræver en kontrol og så videre.

3 Definition. En tredje udfordring er id-nøglen, som ofte er forskellig i forskellige databaser, som beskriver samme område. En nøgle i en database er en unik værdi, som kun repræsenterer et objekt.

Virksomheder har ofte forskellige nøgler i en kundedatabase og en leverandør-database. Arbejdet med at samordne dem kaldes master data management. Der kan være nødvendigt både i beslutningsstøtte og transaktionsanvendelse, eksempelvis ordresystemer. Der er flere mulige løsninger på problemet.

I et transaktionssystem kan man have en separat database, som holder styr på, hvilke forskellige nøgler, der repræsenterer samme objekt. Den database, "master-databasen", kaldes, når en transaktion udføres.

I en beslutningsstøttedatabase kan man forestille sig, at nøgler konverteres, så kun en af dem anvendes til et objekt. Det kan betyde, at det går mærkbart hurtigere at foretage analyserne.



Fem ting man skal have styr på

Dårlig datakvalitet fører til mange problemer, store som små. Her er fem eksempler på, hvad du skal være opmærksom på.

- 1 Hvis datterselskaber i en koncern har forskellige id-nøgler i en kundedatabase, og der ikke er nogen information, der knytter dem sammen, bliver det svært at få et billede af, hvordan hele koncernen er som kunde.
- 2 Hvis datoer er forkerte eller mangler i en database over sælgerbesøg, kan man ikke få en korrekt statistik over, hvordan sælgerne arbejder. Dermed er der risiko for, at sammenligninger mellem forskellige afdelinger bliver forkerte.
- 3 Hvis brugere, som registrerer data, skal angive kategoriværdier som fritekst, kan man ikke sammenligne informationerne. Rækker i en tabel, som egentlig tilhører samme kategori, vil ikke fremstå som sådan.
- 4 Hvis man satser på de funktioner for ugenummer, som ligger indbygget i databaser fra amerikanske leverandører, giver det garanteret fejl på vore breddegrader. Amerikanske ugenumre er ikke de samme som vores.
- 5 Hvis tiden er registreret i form af tre almindelige tal for time, minut og sekund, bliver det kompliceret at foretage tidsberegninger. Nu om dage kan de fleste databaser og andre værktøjer regne med information, som angives som tidsangivelser. Der er ingen grund til at dele tidsangivelsen op i time, minut og sekund.

6. Sikkerhedsprogrammer – sådan fungerer de

Man kan godt opbygge en god basal beskyttelse med programmer og tjenester, selv om man ikke kan beskytte sig mod målrettede angreb. Her er softwaren og det, du bør tænke på.

Det kan du købe

1 Firewalls overvåger trafik til og fra en computer og stopper skadelig trafik. Har man en pc, er der en firewall indbygget i Windows, og mange pc'er leveres med prøveperioder til antivirusprogrammer.

2 Antivirusprogrammer leder efter virus på en computer, enten når man sætter den i gang med en opgave eller løbende. I prøveperioden til antivirusprogrammer indgår opdateringer af virusdefinitioner, senere må brugeren selv betale

3 Avancerede sikkerhedsprogrammer. Der findes flere forskellige typer sikkerhedsprogrammer, for eksempel anti-spionprogrammer, som finder og fjerner kode, som overvåger og sender brugerens kommandoer videre. Der findes også programmer, som holder øje med, om webservere dirigeres om til skadelige websteder. Desuden findes avancerede programmer, en slags super-firewall, der også beskytter mod indbrud.

Det skal du tænke på

1 Lokalt eller netværk? En variant er, at sikkerhedsprogrammer køres lokalt på en klient-pc eller en server, en anden at de køres i et netværk, hvor en computer overvåger alle computere i netværket samt trafik i, til og fra det.

En tredje type er webtjenester, altså at en server på internet tager sig af sikkerhedsarbejdet.

"Hver eneste computer, som er sluttet til andre computere, skal kunne stå på egne ben. Der har været for stort fokus på de netbaserede beskyttelsesmetoder, siger Thomas Nilsson, grundlægger og medarbejder af it-sikkerhedsvirksomheden Certezza.

Han mener, at der er et behov for netbaseret beskyttelse, men at det skal ses som et supplement til sikkerhedsprogrammer, der kører på den enkelte computer, fordi der er behov for forskellige typer beskyttelse.

"En firewall er en udmærket beskyttelse i de lavere kommunikationslag, men betydeligt dårligere i de applikationsnære lag.

2 Tro på dig selv. "Opbyg et grundlæggende hygiejeniveau ved hjælp af gratis sikkerhedsprodukter som antivirus og firewall og invester de penge, som ellers ville være gået til licenser, på eksperter," anbefaler Predrag Mitrovic, chef for Labcenter i Stockholm.

Predrag Mitrovic mener, at man med den strategi satser mere på egne kompetencer end på fine ord fra leverandører, som måske fremmer deres egen sag.

Med hensyn til hvad næste gennembrud for sikkerhedsprogrammer bliver, er han helt sikker:

"Små, specialiserede programmer og tjenester i stedet for mastodontprojekter".

3 Æg eller løg? Per Hellqvist, specialist i it-sikkerhed i Symantec, definerer to scenarier for, hvordan man kan bruge sikkerhedsprogrammer.

Ægsikkerhed er, når man lægger al sikkerhed i gateway-miljøet, altså i ens eget nets berøringspunkter med omverdenen.



Løgsikkerhed er, når man har lag på lag af forskellige sikkerhedsprodukter, som betragter sikkerhed fra forskellige synsvinkler.

”Desværre har for mange virksomheder al sikkerheden i gatewayen. Med løgsikkerhed opbygger man en mere robust sikkerhedsløsning,” mener Per Hellqvist.

Beskytter ikke mod det hele

Sikkerhedsprogrammer er fyldt med sikkerhedshuller og virusdefinitioner, der er lette af aflure. Stol ikke blindt på produkterne.

Et sikkerhedsprogram, som fanger alle trusler, ville være som en målmand, der aldrig lukker et mål ind. Ingen af dem findes.

Blandt sikkerhedsprogrammerne er det ofte antivirusprogrammerne, der får kritik. Kritikken gælder blandt andet, at de kræver mange systemressourcer, og at det er svært at foretage indstillinger i brugerversionerne af dem.

Samtidig rettes der kritik mod, at programmerne for en stor del baserer sig på virussignaturer, altså definitioner af virus som allerede er blevet opdaget.

I mange tilfælde er det enkelt at ændre i et virus, så signaturen ikke længere kan bruges til at identificere den.

En måde at komme om ved problemet er at ændre strategi for sikkerhedsarbejdet. I stedet for at forsøge at identificere kendte vira og mistænkelig opførsel for de programmer, som kører, kan man sørge for, at kun godkendte programmer kører. Den strategi kaldes white listing eller hvidlistning.

Per Hellqvist arbejder i Symantec, der leverer sikkerhedsprogrammer. Når han bliver spurgt, om hans arbejdsgiver og andre leverandører gør arbejdet med sikkerhedsprogrammer godt, er han ikke i tvivl:

”Ja det gør vi i Symantec. For at møde dagens foranderlige trusler, sørger vi for at levere sikkerhedsløsninger med en kombination af forskellige teknikker, som opdateres automatisk”.

Alle sikkerhedsekspertter, som Computerworld har talt med, fremhæver, at det handler om en kombination af teknik, de der håndterer den, og de der arbejder i de miljøer, der skal beskyttes.

”Det er ligegyldigt, hvilken firewall eller hvilket antivirus-program man bruger, hvis man lader computeren ligge i bilen, når man går i biografen, siger Per Hellqvist.

CRM On Demand

- ✓ #1 In CRM
- ✓ Pre-Built Integrations to ERP
- ✓ Tailored By Industry
- ✓ Private Database Option

Oracle Customer Relationship Management
Over 4.6 Million Satisfied Users

ORACLE®

CRMOnDemand.Oracle.com
or call 1.866.906.7878