

Bakgrunnsnotat

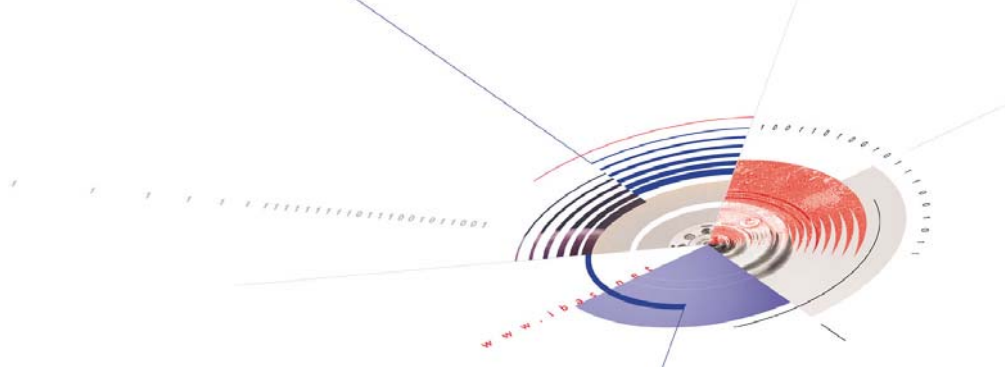
Ibas / NorSIS undersøkelse august 2007:

Skremmende dårlig kunnskap om sletting av data

Visendi har på oppdrag fra Ibas og Norsis gjennomført en representativ undersøkelse blant 100 IT-sjefer i bedrifter med mer enn 100 ansatte og 200 bedrifter innen SMB. Dette er et publikum som burde være de mest bevisste i Norge når det gjelder datasikkerhet. Allikevel viser undersøkelsen at store mengder personlige og forretningskritiske data kan være på avveie i Norge.

Undersøkelsen avdekker betenkelig mangel på fokus på nødvendigheten av riktig sanering av utrangert datautstyr. Her er noen av hovedpunktene i undersøkelsen.

- Hver fjerde norske bedrift med mer enn 100 ansatte har unnlatt å slette data ved utskiftning av datautstyr det siste året
- 1 av 3 av bedriftene som ikke slettet data, sier dette ikke skyldes en spesiell grunn
- 17 prosent sier de ikke hadde tid til å foreta sikker sletting
- Hele 98 prosent sier i tillegg at de har sensitive eller konfidensielle data lagret i bedriften. Situasjonen blir ikke mindre urovekkende når seks av ti virksomheter med mer enn 100 ansatte sier de skal bytte datautstyr det nærmeste halvåret
- 1 av 3 norske bedrifter sletter data ved hjelp av formattering. – Formattering fjerner ikke dataene, du fjerner kun innholdsfortegnelsen
- 1 av 2 bedrifter ødelegger harddisken fysisk, en metode som verken er miljømessig eller samfunnsmessig riktig da mange offentlige funksjoner mangler PC-er
- 1 av 4 bedrifter i Norge med mer enn 100 ansatte leaser datautstyr. 70 prosent av disse aner ikke hva som skjer med dataene når utstyret returneres etter endt leasingperiode til leverandøren.
- 1 av 3 SMB'er oppgir at de tillater at defekte lagringsmedier sendes til garantibytte uten at data er slettet
 - Verst er situasjonen blant SMB'er med 50 – 99 ansatte, der drøyt halvparten (53,1 prosent) tillater at denne praksisen



Ibas' erfaringer

Ibas opplever, igjennom vår kontakt med private og offentlige virksomheter, at praksis i forhold til datasikkerhet er meget varierende. En del har tilfredsstillende rutiner, men mange praktiserer meget liten grad av databeskyttelse - både i forhold til innsyn i og sikring av data. Svak datasikkerhet gjør private bedrifter, organisasjoner og offentlige virksomheter og institusjoner mer sårbare. I ytterste konsekvens truer det i enkelte tilfeller også personvernet.

Generelt om datasletting

Få er klar over at det er nesten umulig å fjerne all informasjon på en harddisk med den struktur og oppbygging som dagens operativsystemer har. "Format", "fdisk" og slettekommandoer fjerner faktisk ikke informasjon som er lagret på din datamaskin. Disse kommandoene bare endrer strukturen på disken, og lar det meste av dataene være intakt og mulig å rekonstruere med tilgjengelig programvareverktøy. Gjennom vår virksomhet kjenner vi til profilerte selskap som ikke tar noen sjanser, men som angivelig skal ha senket harddisker ute i Oslofjorden for å forhindre at noen skal få kjennskap til innholdet.

Datasletting = økt sikkerhet

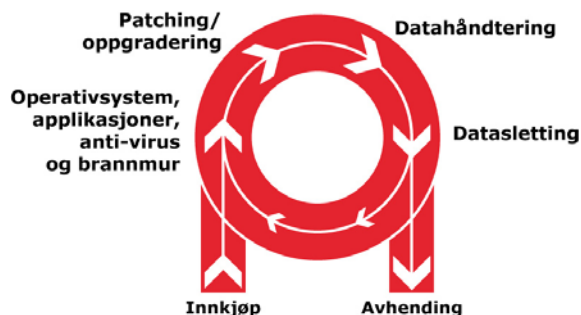
Når du forsikrer huset ditt mot brann, er det ikke fordi du tror huset kommer til å brenne, men for å sikre deg hvis det mot formodning skulle ta fyr. Datasletting fungerer på samme måte. Visendi undersøkelsen viser også at 55 prosent av alle bedrifter har rutiner for sletting av data. De forsikrer seg om at data ikke skal komme på avveie når de avhender en datamaskin.

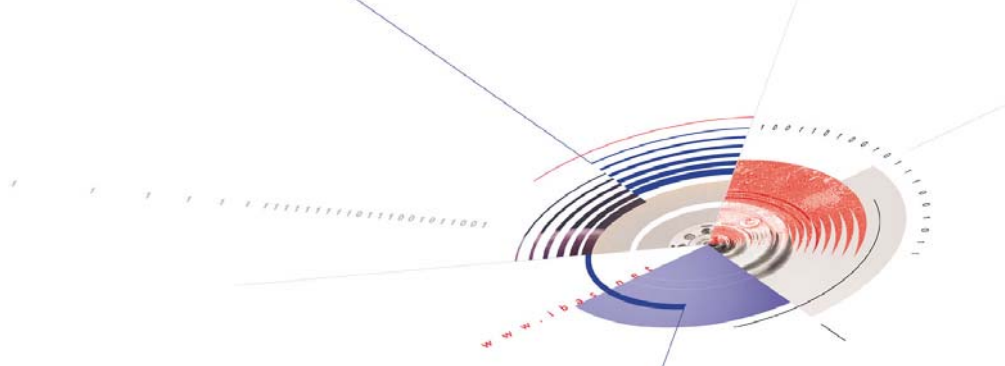
Som en naturlig del av bedriftens totale sikkerhetsrutiner, velger stadig flere Ontrack Eraser Software. Det er en rimelig forsikring som gir garantert resultat og kan spores til den enkelte enhet som er slettet. Prisen for profesjonell og sikker sletting er svært lav, spesielt sett i forhold til kostnaden hvis data skulle komme på avveie.

Hold helt til mållinja

Sikkerhet er viktig fra anskaffelse til avhending. Det er utrolig hvor mye tid og ressurser IT-avdelingen kan legge i datasikkerhet, for så å glemme det fullstendig når PC-en skal kastes, selges eller gis bort. Det hjelper ikke hvor godt du er beskyttet av brannmurer, anti-virus og nettverkspassord hvis du gir bort PC-en med alle data lett tilgjengelig på harddisken. Selv om alle filene er lagt i papirkurven og harddisken er formattert, er det en smal sak å finne dem frem igjen for en profesjonell informasjonsjeger.

Du kan selvfølgelig finne frem slegga og knuse harddisken, men det er både dyrt og lite praktisk. Samtidig er det lite miljøvennlig å knuse noe som faktisk kan resirkuleres og komme andre til gode. Formatterer du harddisken, kan det sammenliknes med å rive ut innholdsfortegnelsen i en bok. Hvis du vil sørge for at riktig person har tilgang til riktige data, bør du levere fra deg PC-en i den tilstanden den kom – uten noen av dine data på den.





Fem vanlige slettemetoder – og én sikker metode

Følgelig er datasikkerhet mer enn antivirus, brannmurer og interne sikkerhetsrutiner. Når det gjelder sikker sletting, finnes det en rekke måter å "slette" data fra et medium på som er utbredte i dag. Men ingen av dem garanterer at informasjonen blir borte for godt.

1. "Vanlig" sletting av filer ikke nok

Del-kommandoen oppdaterer kun en tabell som forteller operativsystemet at filen er slettet. Innholdet av filen eksisterer selv om den jevne bruker ikke kan få den frem.

2. Formatering

Formateringskommandoen oppdaterer tabeller som sier at alle filer og kataloger er slettet, men fjerner ikke data fysisk fra mediet.

3. Overskriving med software

Det er vanskelig å garantere at data fysisk er overskrevet. En bruker kan ikke kontrollere når og hvor data lagres på mediet fordi systemet mellomlagrer. Det er derfor nødvendig å stole på en profesjonell leverandør. Filsletteverktøy sletter kun filer og enkelte partisjoner, aldri hele harddisken.

4. Mekanisk deformasjon

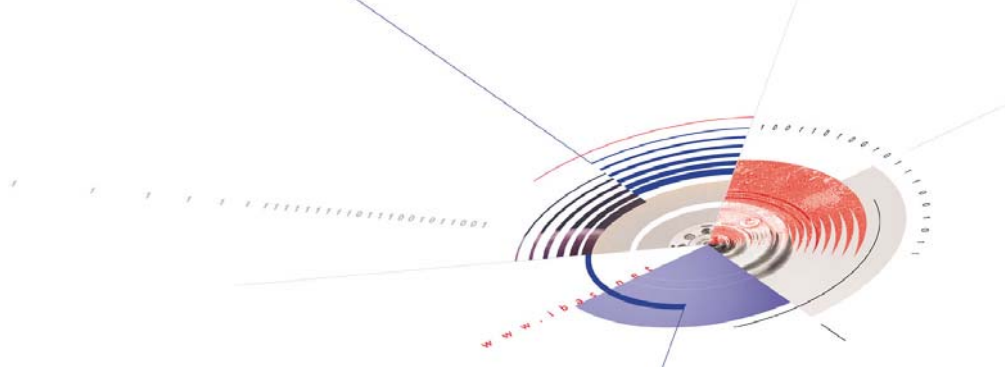
Selv om et lagringsmedium blir knust, er informasjonen fortsatt tilgjengelig. Det er fullt mulig å helt eller delvis hente ut data som ligger på et fysisk skadet medium. Et eksempel på det er at IBAS gjenskapte 90 prosent av innholdet på datamaskinene om bord på den havarerte passasjerfergen Sleipner – etter at harddisken sterkt deformert hadde ligget i saltvann på mer enn 100 meters dyp i flere måneder.

5. Avmagnetisering

Selv om du bruker avmagnetisering for å slette data, er dette ikke alltid tilstrekkelig. Du må vite hvor kraftig magnetfelt som må til, og hvor lenge den spesifikke disken skal utsettes for feltet.

Én sikker metode

Ibas har utviklet ExpertEraser, en programvare som kan brukes til å slette fungerende harddisker. Sletting med denne programvaren er ikke destruktiv og vil på ingen måte ødelegge harddisken. Slettingen består i å overskrive hele harddisken med ugradert informasjon. Dette betyr at all gammel informasjon blir slettet, og harddisken kan gjenbrukes som ny. For sletting av defekte harddisker, taper og disketter har Ibas utviklet en kraftig Degausser. Ved å benytte Degausseren slettes mediet med ett meget sterkt magnetfelt.



Eksempler med data på avveie:

Politimester leverte inn sin hjemme-pc gjennom leasingselskapet. Maskinen havnet på det åpne markedet fullstappet av data bl.a. fra høyt politi profilerte mediasaker samt private bilder, brev og arbeidsrelaterte dokumenter. Personen som kjøpte maskinen på "grå markedet", en mann i tretti årene var rystet over det han kom over.

Apotek 1 i Brumunddal dumpet back up tape på den lokale gjenvinningsstasjonen. Tapen ble funnet av en privatperson som kunne lese ut legejournaler, pasient sensitive data samt legenes aksesskoder for utstedelse av resepter o.l.

Dame kjøpte brukt bærbar pc hos en lokal forhandler, det viste seg at pc-en hadde tilhørt en sykehuslege som byttet den inn for å kjøpe ny. Dataene var forsøkt slettet, men kvinnen kunne med enkle tastetrykk og med ren tilfeldighet komme over legens personlige og faglige data.

Student leverte inn sin pc til garanti reparasjon hos en anerkjent pc forhandler, fikk ny pc og var tilsynelatende fornøyd. Det hun derimot ikke viste var at den gamle pc-en ble reparert, og videresolgt til en annen med bl.a. hennes hovedfagsoppgave...

Politi som benyttet harddisker som blinker på skytebanen

IT-sjefen som pendlet med Nesoddbåten og dumpet harddisker på havets bunn på hjemveien.

5 gode råd ved utrangering av gammelt PC-utstyr:

- Ta stilling til hvordan ønsker du å utrangere maskinen, gi den vekk, brukt salg eller til gjenvinning
- Vurder om det er behov/ønske for å gjenbruke lagringsmediene, dette kan påvirke valg av slettemetode
- Hvis du overlater maskinen til andre, sørg for å få vite hvordan data skal slettes.
- Skaff dokumentasjon på at data **virkelig** blir slettet
- En bedrift eller virksomhet bør etablere en enhetlig sikkerhetspolicy som inkluderer rutiner for sletting av data. Normalt vil pc-er, hjemme-pc-er, kopimaskin, printere, telefaks, PDA, telefon, mobiltelefon og digitalkamera innholde virksomhetens egne data.

Gode råd for hvordan utføre sikker sletting av data:

- Profesjonelle sletteverktøy benyttes for å slette fungerende harddisker sikkert. Avmagnetisering eller såkalte degaussere benyttes ved defekte harddisker, taper eller disketter.
- Sletting via Windows eller sletting vha gratis programvare på Internet gir ikke et godt resultat
- Det er kun sletting av hele harddisken som gir et sikkert resultat, sletting av filer eller partisjoner sletter kun deler av harddisken.
- Operativsystemet som sletteprogrammet benytter må starte opp maskinen får å få tilgang til hele harddisken. Det er ikke viktig hvor mange ganger harddisken overskrives, en gang overskriving holder.
- Et profesjonelt sletteverktøy genererer en rapport ved hver sletting. Dette er dokumentasjon på at din virksomhet ikke har informasjon på avveie