

3-minutters guide

Sterias 3-minutters guide for deg som er opptatt av it og ledelse

www.3-minuttersguide.no



Slik oppnår du økt datasikkerhet

— I 2001 ble 62 prosent av norske virksomheter utsatt for datakriminalitet (kilde: NSO). Trusselen fra hackere og virus er åpenbar, men utro ansatte kan heller ikke utelukkes. Er din virksomhet forberedt på dette? Manglende motiltak kan, i ytterste konsekvens, medføre store økonomiske tap eller uopprettelige tap av anseelse, forteller Lars Venger Gunnarsson, senior rådgiver og en av Sterias fremste sikkerhetsspesialister. Her deler han sin erfaring og gir konkrete tips om hvordan organisasjoner kan oppnå økt datasikkerhet.



Hvordan forebygge mot angrep

Informasjonsteknologien griper inn i alt. Derfor er it-sikkerheten sentral i alle virksomheter. Hvordan kan du planlegge sikkerheten bedre?

Internettet og åpne systemer har økt risikoen for at sensitiv informasjon i bedriften kan endres, mistes eller stjeles. Datasnoker står klare til å bryte seg inn på nettverket ditt. Men mange av usikkerhetene i it-verdenen har også eksistert

tidligere: Utro medarbeidere. Dårlige rutiner. Manglende ledelsesansvar.

Det er viktig å slå fast at it-sikkerhet aldri kan oppnås med teknologi alene. Sikkerheten kan heller ikke basere seg bare på forebyggende tiltak.

La oss dele opp det store temaet på en pedagogisk måte. Arbeidet med it-sikkerhet omfatter fem punkter: Rammebetingelser, risikovurdering, sikkerhetskrav, sikkerhetsperspektiv og metodeverk.

Rammebetingelsene

Det er to ting du bør vite før du begynner å planlegge: Det første er at sikkerhet er vanskelig å legge til i etterkant. Det andre er at 100 prosent sikkerhet er umulig å oppnå.

I dette ligger at datasikkerheten hele tiden er en avveiningssak. Skal man sikre bedre, vil det gå utover brukervennligheten. Det beste eksemplet er kanskje bruken av passord. Bruker medarbeiderne navnet på ektefellen eller hunden for å skaffe seg adgang, er brukervennligheten god, mens sikkerheten er elendig.

Dersom passordet må skiftes fra uke til uke, oppbevares forsvarlig, og er vanskelig å gjette for uvedkommende (f.eks. wxv9879876phXR), er sikkerheten med hensyn til passord antakelig god, mens brukervennligheten kan være dårlig. Bedriften må derfor tenke over hvilket sikkerhetsnivå som er riktig.

Risikovurderingen

En virksomhet som håndterer sensitive opplysninger må arbeide annerledes med it-sikkerheten enn en dagligvarebutikk. Leverandørene i sikkerhetsbransjen har en tendens til å tilby samme løsninger i begge tilfeller, samtidig som de ikke lærer opp kundene sine i hva løsningene er gode for, og hvilke begrensninger de har.

Det syndes også med kompetanseoppbygging i hvordan løsningene skal brukes, og suppleres med rutiner for å opprettholde sikkerheten over tid. Men bedriften bør selv vurdere hvilke risiki som er mest alvorlige, ut fra en verstefallstenkning. Hva ønsker vi å beskytte? Hva er de største farene her? Er det datasnoker

MURBYGGERNE

— Veldig mange it-sikkerhetstiltak i norske virksomheter er basert på at man søker å forhindre at noe skjer, gjerne ved å sette opp en mur rundt datasystemene. Det gir en falsk trygghet. Det er like viktig å verifisere om ting har skjedd, om muren virkelig holder ting ute.

som kan påføre bedriften mest skade? Hvilke metoder har de til rådighet? Er det egne medarbeidere? Hvilke metoder har de til rådighet? Hva hvis hovedsystemene faller ut - hvor fort kan bedriften legge sikkerhetskopiene inn? Hvor lenge kan it-systemene være satt ut av spill før det blir kritisk for hele virksomheten?

Sikkerhetskravene

It-sikkerhet bør ikke baseres på synsing. Arbeidet må ha et rammeverk. Det finnes flere egnede standarder, for eksempel ISO/IEC 17799, som peker på de områdene det med fordel kan legges mer vekt på i de fleste bedrifter.

Sikkerhetskravene må gjøre det mulig å fange opp også det uventede. Forbausende mange bedrifter er for eksempel ikke klar over at det skjer datainnbrudd. Det finnes ikke mekanismer og prosedyrer i virksomheten som er i stand til å fange opp denne typen problemer, fordi ledelsen ikke har vært klar over dem. I noen bedrifter er man pålagt lover og retningslinjer. I de fleste må det utvikles egne, definerte krav.

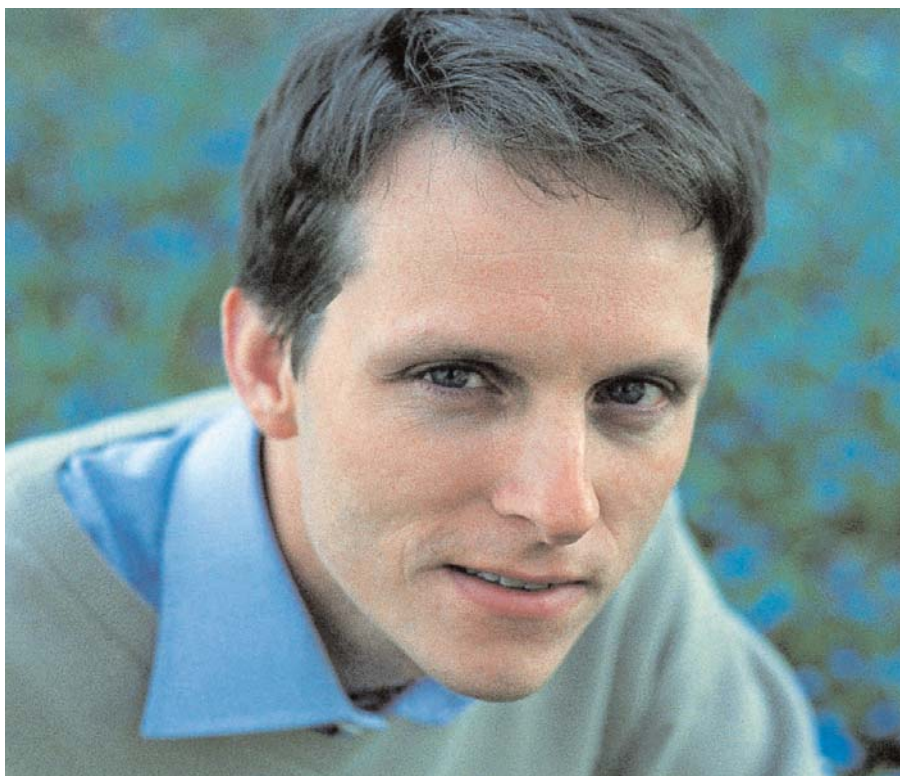
Sikkerhetsperspektivet

For noen virksomheter er stikkordet «sikkerhet» så entydig og snevert definert at de tyr til like entydige løsninger: Bedriften kjøper en rød boks med til-



ER DU SUGEN PÅ KUNNSKAP?

Har du vært innom www.steria.no? Adressen bør du merke deg. Her finner du mye nyttig stoff for ledere som tar it og ledelse på alvor.



hørende programvare. Så sier ledelsen at «vi har løst problemet. Vi har it-sikkerhet!». Dette perspektivet ligner ideen om at «når vi bare har medisinskap, trenger ingen i denne bedriften førstehjelpskurs». Men teknologi alene kan aldri løse alle problemer. Generelle sikkerhetsapplikasjoner kan i noen tilfeller dekke over hva som faktisk er vesentlig.

Veldig mange tiltak i en bedrift er basert på at man søker å forhindre at noe skjer, gjerne ved å sette opp en mur rundt datasystemene. Det brukes mindre ressurser på å verifisere om ting har skjedd, om muren virkelig holder ting ute.

Det eneste riktige perspektivet for sikkerhetsarbeidet er å være forberedt - alltid. Det vil si å ha et øye til både prosesser, systemer, rutiner, policy, opplæring og dokumentasjon.

8 viktige huskereglene

- It-sikkerhet er ikke it-avdelingens ansvar. Det er ledelsens. I tillegg til å ha det økonomiske ansvar, har den også et juridisk ansvar for at informasjon lagres, sikres og gjøres tilgjengelig i overensstemmelse med lover og regler.
- Ting kan alltid gå galt. Ingen sikkerhetsløsning er fullgod. Nøkkelen til en fornuftig ordning er å sette inn tiltak på de mest kritiske områdene, ellers kan du fort ende opp med en dyr forsikring.
- Mange typer datainnbrudd blir aldri oppdaget - fordi bedriften ikke ser

etter dem. Sørg for å se etter dem - regelmessig!

- Selv «harmløs» datasnoking kan være skadelig. Enkelte it-systemer er svært skjøre. Systemets integritet kan være ødelagt dersom en ikke-autorisert person kommer seg inn.
- Finnes det verdier, finnes det også kjeltringer. It-svindler er kommet for å bli, særlig overfor systemer som kan gi økonomiske gevinster.
- Sats ikke bare på forebyggende tiltak. Enda viktigere er det å tenke gjennom hva bedriften skal gjøre hvis det skjer brudd i sikkerheten.
- Trusselen fra hackere er åpenbar. Se heller ikke bort ifra utro ansatte. Akkurat det er mye farligere enn hvis utenforstående prøver seg.
- Datasikkerhet kan aldri oppnås bare ved kjøp av nye bokser og dataprogrammer.

KONTAKT

Lars Venger Gunnarsson,
senior rådgiver, Steria AS
e-post: lvg@steria.no
Tlf. 22 57 57 04. Mobil: 992 48 805
Steria AS, Biskop Gunnerus' gate 14A,
Pb. 2, N-0051 OSLO