

Skyt pianisten!

Å feile i forhold til ambisjoner, krav eller målsettinger kan håndteres på mange måter. Den minst effektive – men like fullt mest alminnelige metoden, ikke minst her til lands, er å finne noen å skylde på, og deretter toe sine hender.

Denne begredelige tradisjonen ble vi minnet om da vi forleden leste om ISPenes påståtte sikkerhetsansvar i en herværende IT-publikasjon: Redaktøren mener at nå må Internett-leverandørene skjerpe seg! Det er deres ansvar å sørge for at virus og annen styggedom ikke finner veien inn i kundenes nettverk. Alternativt må kundene se seg om etter andre leverandører som er seg sitt ansvar bevisst, tordner redaktøren videre. Noen dager senere hadde andre plukket opp tråden og fortsatte på det samme tankeløse sporet.

Vi gremmes. Forstår de virkelig så lite av verden vi lever i, mangler evnen til å tenke selv, eller har de rett og slett gått tomme for stoff? Hvorfor ikke samtidig anklage Vegdirektoratet for å forsømme sine oppgaver i og med at forbrytere kjører rundt på våre veier? Så hinsides er tanken om at innholdskontroll av all trafikk skulle være ISPenes ansvar.

Ikke bare er slik kontroll så godt som umulig, i alle fall om vi stiller rimelige krav til effektivitet. Det er lett å se for seg det resulterende kaos om veimyndighetene stanser all trafikk på E6 i sin søken etter forbrytere. Enda et hakk verre er imidlertid tanken på at noen skulle ha rett – for ikke å snakke om plikt – til å studere all trafikk. Tillit er viktig og nyttig, men en slik overvåking ville få Huxleys BRAVE NEW WORLD til å virke som et paradisi.

Heldigvis er det få som har tatt tåpelighetene alvorlig. De har havnet der de hører hjemme – i glemmeboken. Imidlertid dukker saken opp i erindringen når vi i disse dager leser om ISPer som virkelig tar sin oppgave og sitt ansvar på alvor. Siste års DENIAL OF SERVICE angrep, som ble muliggjort av feil i Microsofts programvare og driftsmiljøer som unnlater å holde sine systemer oppdaterte, satte en støkk i de aller fleste. Angrepene lammet hundrevis av ISPer og tusenvis av andre miljøer over hele verden – inklusive Microsoft selv – i flere dager.

ISPene kan ikke kontrollere trafikken, men de kan stille krav til sine kunder – på samme måte som kundene stiller krav til dem. Generell sikkerhet er minst like viktig for en ISP som for andre IT-miljøer. Faren for smitte når infeksjoner og virus dukker opp, er spesielt fremtredende i et miljø som håndterer stor trafikk og huser postkasser for hundrevis eller tusenvis av kunder.

Derfor er det kanskje underlig at ISPene ikke har snudd seg mot kundene med skikkelige krav til god hygiene for lenge siden. Under mottoet bedre sent enn aldri, skjer det imidlertid i disse dager. Store amerikanske aktører – som Ameritech, AT&T, CTC, Exodus og EarthLink – går foran, og resten av verden kommer etter. Kravene er omfattende, men likevel selv-



Mellvik-Rapporten® utkommer 11 ganger i året og utgis av:
Team Mellvik as
Postboks 54 Holmenkollen
NO-0712 Oslo
Telefon 22 14 26 47
Telefaks 22 49 35 98
Org.nr. NO 966989351 MVA

Ansvarlig redaktør:
Hanne Mellingen
Fagansvarlig:
Helge Skrivervik
Korrektur:
Kari Mellingen

Epost: info@mellvik.no
URL: www.mellvik.no
ISSN 0804-9386

Særtrykk tilbys, ettertrykk og kopiering forbudt.

Se baksiden for informasjon om abonnement og bestilling av tidligere utgaver.

Mellvik-Rapporten er et registrert varemerke tilhørende Team Mellvik as.

følgelige minstekrav for god sikkerhet: Kryptering, autentisering, anti-SPAM, brannmurer og brannmur-konfigurasjoner, prosedyrer for oppdatering av programvare og så videre. Kunder som ikke vil være med, blir kort og brutalt henvist til å finne seg andre leverandører.

Slik må det være. God sikkerhet har aldri vært viktigere. At de som ikke forstår dette, skal kunne ødelegge for andre er uakseptabelt. For ISPene er forholdet så enkelt som at de ikke kan tillate seg å sette driften i fare. Den som ikke vil han skal, og vi tar av oss hatten for initiativet!

Oslo, 8. november 2001

