

## Sikkerhet på ville veier



Tiden flyr. 16 år har gått siden vi holdt vårt første kurs i nettverkssikkerhet. Uten å henfalle til mimring, er det ikke til å unngå at en før-kontra-nå analyse dukker opp fra tid til annen – for eksempel: Er sikkerheten blitt bedre i løpet av perioden? I motsetning til hva de fleste forventer, er svaret et rungende NEI. Tiltakene vi har utviklet, anskaffet og satt i drift er ikke uten effekt, men de henger etter i kappløpet med risikoer og trusler. Vi har altså brukt milliarder av kroner og andre ressurser uten å ha kommet på offensiven. Tvert imot henger vi stadig lenger etter, ikke fordi den andre siden – fienden, som mange vil kalle det – er smartere, men fordi ressursene brukes feil.

Selv i 2004 er IT-sikkerhet blant de mest misforståtte temaer og fagområder som finnes. Det begredelige faktum er at en person eller en virksomhet ikke trenger å være spesielt smart for å bane seg tilgang til beskyttede systemer og informasjon. En PC, en Internettforbindelse, rudimentær engelsk og grunnleggende kunnskap om søking på nettet er alt som skal til. Der finnes verktøy, oppskrifter og tallrike råd om hvordan gå frem.

‘Aha’ - hører vi fra rekkene. ‘Dette må vi sette en stopper for.’ Dessverre. Feil vinkling. Slik har det alltid vært og slik vil det alltid være. Oppskrifter på hvordan lage bomber og alle tenkelige våpen har vært å finne i biblioteker og på folkemunne siden tidenes morgen. Forskjellen i dag er tilgjengeligheten. Det meste av informasjon er et tastetrykk eller et museklikk unna, sammen med noen som kan trå til med tilleggserfaringer. Dessuten er mulighetene for å utføre ugjerninger av ulike slag uten å forlate kontoret eller hjemmet, enorme.

Feil vinkling er den viktigste årsaken til at vi kaster bort så store summer på sikring og sikkerhet. Symptomer kureres over en lav sko, mens de egentlige sykdommene får leve og spre seg i fred og ro, til stor tilfredsstillelse for utallige selskaper som lever av symptom-kurering – fra leverandører av antivirus-programvare til sikkerhetskonsulenter som rydder opp etter innbrudd og virusangrep.

“En brannmur er en kostbar måte å forsinke nettverkstrafikken på”, sier den kjente sikkerhetseksperter Marcus Ranum, og illustrerer på den måten poenget: Det er ikke mekanismer og bokser som gir god sikkerhet, men forståelse av sammenhengen mellom trusler, risiko og verdier. Mens tusenvis av virksomheter konsentrerer innsatsen om beskyttelse av nettverk og systemer, er det i de fleste tilfeller data og informasjon som trenger beskyttelse. Og dataene befinner seg kanskje på en PDA eller en LAPTOP på en flyplass eller i en bil. Da spiller brannmurer, VPN-forbindelser og PKI liten rolle. Og mens titusenvis av brukermaskiner og tjenere oppdaterer sine virus-signaturer daglig eller oftere, innser de fleste at viruskontroll aldri kan komme i forkant av utviklingen. Virus som ikke finnes, kan ikke sjekkes. Det vil alltid være en forsinkelse på timer, dager eller kanskje uker fra en virus kommer ‘på markedet’ til den er med i de automatiske signaturoppdateringene. I mellomtiden er vi ubeskyttet – åpne for angrep. Akseptabelt? Nei! Uunngåelig? Nei!

Selv etter 16 år streber sikkerhets- og systemansvarlige etter å gjøre sikkerheten usynlig for brukerne. Den skal ikke være i veien, vi må for all del ikke forstyrre

**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](mailto:info@mellvik.no)

URL: [www.mellvik.no](http://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.

brukerne og deres produktivitet. Hørt på maken til vås. Hvor forstyrret blir brukerne dersom vi blir infisert? Hva koster det – i forhold til enkle og synlige tiltak? Har de fleste allerede glemt – overlatt eller uaktsomt – at sikkerhet som ikke er synlig, heller ikke er effektiv?

Om årsaken er kompetansemangel, latskap eller frykt for brukernes vrede er i og for seg uinteressant. Den viktige observasjonen er at sikringsarbeid må over på et annet spor for å bli effektivt. Samtidig kan de fleste organisasjoner spare betydelige ressurser. At det i prosessen må spises kameler over en lav sko, er også en del av helheten. Men hva er vel en kamel i forhold til god IT-sikkerhet og lavere kostnader? Et enkelt valg. Her er litt hjelp på veien:

- ✘ Sikringstiltak som ikke er synlige, er ikke effektive.
- ✘ Sørg for at brukerne blir medarbeidere, ikke motarbeidere. Brukerne er ikke mot god sikkerhet, de er mot tiltak og plager de ikke forstår.
- ✘ Finn ut hva som skal beskyttes og hvorfor. Anvis deretter tiltakene.
- ✘ Kurerer av symptomer gir aldri langvarig effekt. Konsentrér innsatsen om spredningsmekanismene, ikke om hvert enkelt virus.

Oslo, 2. juni 2004

