

Sikkerhet: Hvem er fienden?



Situasjonen er ganske bisarr: Det finnes ikke mange virkelige crackere – datasnoker – i verden. Kanskje et hundretalls personer har kompetanse og innsikt nok til å lage gode virus og programmer/verktøy som skaffer urettmessig adgang til systemer. Vel er det slik at programvare generelt er fullt av hull og svakheter, men det er også et faktum at det skal betydelig ekspertise til for både å finne og å utnytte dem.

Det bisarre er at dette knippet innsiktsfulle, malignante 'håndverkere' driver en hel industri: Det omsettes beskyttelses-programvare og verktøy for milliarder av dollar år om annet, mens den egentlige fienden er et beskjedent antall personer. Men hva mener leverandørene av slik programvare om dette forholdet? Om vi spør dem, mener de utrolig nok ingen ting. Dette er deres levebrød, de lever av å kurere symptomer, og er egentlig ikke interesserte i den dypere årsak til problemet. Det har riktignok alltid vært slik at den enes død er den andres brød, men den situasjonen vi har i dag er på grensen til det absurde. Er det rart media fra tid til annen lurer på om det er programvareleverandørene selv som finansierer utviklingen av nye virus? Vi skal vokte oss vel for å støtte en slik teori, men vi har samtidig vanskelig for å kalle antivirus-bransjen for seriøs: Den er rett og slett for lite opptatt av det grunnleggende problemet. Hvordan ville vi ha reagert om vi fikk vite at en lege eller veterinær notorisk behandlet symptomer i stedet for å ta tak i den underliggende sykdommen?

Crackere er imidlertid ikke den eneste IT-relaterte trusselen vi står overfor i hverdagen. Parallelt med at vår avhengighet av IT-verktøy og systemer vokser, øker naturlig nok attraktiviteten for alle typer kriminelle – og kriminalitet. Blant de mindre opplagte variantene i bildet finner vi kombinasjonen OUTSOURCING/mafiavirksomhet. Neppe en overhengende trussel på våre breddegrader i overskuelig fremtid, men aktuelt for internasjonale selskaper, og dessuten vel verdt å tenke gjennom: OUTSOURCING betyr å gjøre seg avhengig av noen – det være seg energiverket, tele-leverandøren, Internett-leverandøren eller andre tjenesteleverandører. Jo flere tjenester som havner på én hånd, desto større er avhengigheten, og tilsvarende stor blir partenes muligheter til å misbruke forholdet.

Langt mer innpå livet for oss alle er det forhold at våre medarbeidere alltid representerer vår største sikkerhetstrussel. Bedre blir det ikke av at de fleste toppledere – faktisk ledere generelt – ikke er klar over dette enkle faktum. De stikker hodet i sanden hver gang temaet kommer opp, og holder det der lenge nok til at 'faren' er over. En slik neglisjering av virkeligheten er langt alvorligere enn å droppe forsikringene i håp om at det aldri blir bruk for dem. Sammenligningen er imidlertid ikke ueffen: Det er en grunn til at enkelte forsikringer er lovpålagt, for eksempel i forbindelse med motorkjøretøyer.

Det er rimelig å forvente en annen innstilling til ansvar og innsikt i virksomhetenes egentlig behov – fra ledere på alle nivåer. "Ute av syne, ute av sinn" er i beste fall en elendig ledelsesfilosofi, i verste fall en snarvei til katastrofe.

Over 80% av alle norske virksomheter mangler både en grunnleggende sikkerhetspolicy, elementær katastrofeberedskap og konkrete (skriftlige) hold-

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.

ninger til bruk av moderne kommunikasjonsverktøy – fra epost til mobiltelefoner. Blant de resterende 15-20% mener halvparten å ha gjort noe med problemstillingene, men er i virkeligheten akkurat like langt: De er i besittelse av policies og dokumenter ingen kjenner til, som er gått ut på dato eller er skrevet av personer uten innsikt i de egentlige problemstillingene. Dette er verre enn å stå på bar bakke – unnskyldninger for ikke å foreta seg noe.

I vår virksomhet som sikkerhets-rådgiver for store og små virksomheter de siste årene, har vi sett utallige eksempler som dekker hele spekteret. Den eneste lysningen på horisonten er en gryende bevissthet om at det ikke kan skure lenger. Om noe positivt har kommet ut av terrorhandlingene i USA 11. september 2001, så er det et kraftig dytt i ryggen for denne bevisstgjøringsprosessen. Bevissthet – om ansvar, trusler og virkelighet – er første trinn. Handling er det neste.

Hvem fienden er? Først og fremst ledelse og ledere som ikke tar ansvar. I andre rekke medarbeidere som ikke kjenner sin egen rolle i sikkerhetsbildet. Først i 3. rekke kommer all verdens snoker og crackere – proffene, kopistene og amatørerne. Vanskelig å prioritere? Nei, tvert imot!

Oslo, 13. januar 2002

