

Til kamp mot CyberCrime

At kriminelle elementer og vandaler nærmest uten unntak ligger et hestehode eller to foran ordensmakt og andre som arbeider med sikring, er en naturlov. Beskyttelsestiltak er alltid reaktive i den forstand at de først blir satt i verk etter at trusselen er et faktum. Uansett hvor gjerne vi skulle ønske at virkeligheten var annerledes, er denne rekkefølgen like selvfølgelig som tyngdekraften. Vi kan ikke beskytte oss mot trusler som ikke finnes. Ei heller kan vi forutse all vedens tenkelige trusler.

For eksempel: Ingen andre enn et par kreative *science fiction* forfattere antesiperte datavirus før de var et faktum. Derfor fantes det heller intet forsvar mot dem. Analogien mot den medisinske siden er stadig like god: Vaksine mot sykdommer ingen har oppdaget – eller forårsaket, finnes ikke.

Katt og mus

Kort og godt er det slik at vi må kjenne til en fiende før vi kan sette i gang forsvarstiltak. Når fienden er identifisert og har gjort sine første fremstøt, har vi forutsetninger for å kunne analysere angrepene og utarbeide forsvarsstrategier. Men har vi ressursene som skal til?

Svaret er – dessverre – et rungende nei. Uansett hvilke menneskelige, tekniske og økonomiske ressurser som settes inn, vil forsvarsaktivitetene være handicappet på grunn av tidsmangel: Det blir aldri tid nok til å kunne holde oppe et aktivt forsvar og samtidig forutsi og planlegge hva som kan bli motstanderens neste trekk.

På grunn av tidsmangel og utilstrekkelig tilgang på andre ressurser, er de fleste sikringsaktiviteter – innen IT og på andre områder – reaktive, kun unntaksvis proaktive. På IT-siden ser vi at såkalte Crackere¹ – ungdommer som primært vil demonstrere sin dyktighet, eller regulære forbrytere – har mye av nettopp den ressursen forsvarerne mangler mest: Tid. Dessuten står de overfor et høyst ujevnt – i mange tilfeller fraværende – forsvar.

Vi kan bevilge mer tid og andre ressurser, men tyngdekraften får vi aldri gjort noe med – og ei heller den menneskelige natur. Et effektivt forsvar som kontinuerlig tilpasses en virkelighet i forandring, er derfor nødvendig – kombinert med varslingsystemer som minimaliserer sjansene for at inntrengere kan passere inn og ut av våre systemer uten å bli oppdaget.

De militære analogiene er tallrike og nyttige: Oppgaven er å finne effektive vinklinger på forsvaret, å maksimalisere nytteverdien av de

¹ Betegnelsen 'Hacker' blir ofte benyttet i samme betydning som 'Cracker'. 'Hacker' er imidlertid opprinnelig en positiv betegnelse – på en dyktig, gjerne ung og ofte asosial programmerer, og vi bruker konsekvent 'Cracker' i denne artikkelen.

ressursene som finnes, og gjøre det både vanskeligere og mer ressurskrevende å trenge gjennom forsvarsverket.

Det er innlysende at dårlig eller fraværende forsvar er fullstendig uakseptabelt og uansvarlig. En slik situasjon inviterer Crackere til målet som fluer til en fersk hestelort. Ryktene om åpne dører og vinduer sprer seg raskere over nettet enn vinden blåser, og konsekvensene er i beste fall kostbare, i verste fall katastrofale.

Et sterkere forsvar

Å heve nivået – styrke forsvaret – er første prioritet, et kjent faktum for Mellvik-Rapportens lesere, men hvor skal vi begynne og hvordan skal utfordringen angripes? De fleste velger letteste vei ut: Å kontakte en leverandør, evaluere produkter og sette dem i bestilling. Tiltakene fører imidlertid i beste fall til bedre sikkerhet over en kort periode: Innkjøp av 100 jagerfly bedrer ikke den norske forsvarsevnen før pilotene er på plass, godt trent, i beredskap og inkorporert i en total forsvarsstrategi. Dessuten er det slik også i IT-sammenheng at forsvaret er lite verdt uten et varslingsystem som gir et minimum av tid til å forberede spesifikke angrep – og et minimum av kunnskap om trusselens beskaffenhet.

Kunnskap, innsikt og varslingsystemer er med andre ord nøkler til den nivåhevingen vi er ute etter. Det betyr samarbeid, på tvers av industrier, bransjer, landegrenser og kontinenter, kombinert med effektive lokale tiltak. Og ikke overraskende, kommer initiativer i den retningen fra USA, der utfordringene er størst og tilgangen på ressurser best.

En rekke varslingscentre som koordinerer informasjonsflyten i forbindelse med innbrudd, virus, ormer og så videre, er etablert de siste årene – med tilhørende aksjonsgrupper bestående av eksperter fra industri, utdannelses- og forskningsinstitusjoner. Disse har primært lokalt fokus, og blir drevet med full eller delvis finansiering fra det offentlige. Betydningen av 'lokalt' i en verden der en jordomseiling tar mindre enn et sekund, er imidlertid i beste fall vag, og behovet for å globalisere innsatsen har blitt stadig mer påtrengende.

The Internet Storm Center

The Internet Storm Center (ISC), som ble etablert høsten 2000, kjenner ingen geografiske grenser og har som målsetting å samle kunnskap om, varsle og bidra til bekjempelse av programbasert Internett-kriminalitet.² Angrepsvinkelen er interessant – inspirert av et annet globalt og i mange tilfeller truende fenomen: Været. Ved å benytte tanker, ideer og metoder fra internasjonal værvarsling, har ISC i løpet av kort tid kunnet etablere en global varslings-tjeneste for angrep via Internettet. Kostnadene er beskjedne, og den løpende overvåkingen foregår innenfor rammen av det vi kan kalle moderorganisasjonen, SANS Institute, som også er initiativtaker til tjenesten. Det globale informa-

² Programbasert betyr at aktivitetene fokuserer på alle slags programmerte trusler: Virus, ormer, trojanske hester, DENIAL OF SERVICE (DoS) verktøy og så videre, og forsvar mot disse.

sjons- og varslingsystemet som er etablert, baserer seg på frivillighet og utnytter det faktum at tjenestene er like nyttige for alle som deltar: Det kommer mer ut enn noen setter inn. Dermed er det lett å argumentere for deltagelse – et faktum tusenvis av organisasjoner over hele verden har innsett.

Bakgrunn

Utover den situasjonen vi beskrev innledningsvis, ble etableringen av ISC trigget av det faktum at organisasjoner flest synes å være ute av stand til å håndtere innbrudd og andre sikkerhetsrelaterte problemer på en effektiv måte. Situasjonen kan eksemplifiseres slik:

Til tross for store investeringer og andre tiltak på sikkerhetsfronten, forekommer innbrudd. Ingen overraskelse for oss som arbeider med sikkerhet, men vanskelig å forstå og å forklare for en toppledelse som trodde foretatte investeringer hadde løst problemet en gang for alle. De involverte snur seg rundt og leter etter noen å skylde på. Toppledelsen registrerer at prosessen ikke fungerer, sparker lederen, ansetter en ny, og beordrer en omorganisering. En mengde svakheter oppdages. Situasjonen krisemaksimeres, midler avsettes og en ny sikringsprosess er i gang. Prosessen tar tid, typisk flere måneder i stedet for de 2-3 ukene toppledelsen ser for seg. Innen den er ferdig, har nye trusler dukket opp som ikke er dekket av tiltakene, og et nytt innbrudd skjer. Alle involverte snur seg rundt og leter etter noen å skylde på ... og så videre. Hele prosessen gjentar seg.

Beskrivelsen kan være satt noe på spissen, men det er innlysende at selv en moderert utgave neppe noen gang vil gi tilfredsstillende sikkerhet. Problemet må angripes på en annen måte – og nettopp denne erkjennelsen ligger til grunn for *The Internet Storm Center*: Tilstrekkelig mange organisasjoner kjente seg igjen i prosessbeskrivelsen ovenfor til å ønske initiativet fra SANS Institute velkommen. Ved å samle kreftene mot en felles fiende, var det innlysende at situasjonen kunne forbedres vesentlig, kanskje tilstrekkelig til å besørge en reversering av den truende bølgen.

Hvordan

Metodikken er hentet direkte fra meteorologene: Enkle 'programvare-agenter' eller 'sensorer' – små programmer – på så mange steder som mulig, filtrerer relevant trafikkinformasjon og sender den til et regionalt senter. Her sammenstilles dataene før de videreformidles til et såkalt koordineringssenter under kontroll av *Internet Storm Center*. Ved hjelp av denne informasjonen kan senterets analytikere, som alltid er på vakt, i løpet av noen minutter oppdage 'stormer' underveis – det være seg angrep som er under oppbygging eller virus som er under utvikling.

Lion-viruset (egentlig en såkalt orm) fra tidligere i år, ble senterets svenneprøve og demonstrerer hvordan systemet fungerer i praksis: Den 22. mars viste sensorer fra enkelte deler av verden økt trafikk på 'port 53' – som i klartekst betyr trafikk knyttet til navneoppslag i Inter-

Noen av organisasjonene som deltok i å få *Internet Storm Center* i gang:

- National Institute of Standards and Technology (USA)
 - Infocomm Development Authority of Singapore
 - Naval Surface Warfare Center
 - US Treasury Financial Management Service
 - Washington State Dept. of Health
 - NASA
 - Australian National Audit Office
 - US Dept. of Justice
 - Royal Canadian Mounted Police
 - Communications Security Establishment (Canada)
 - Canadian CERT
 - VISA
 - Union Bank of California
 - Nat'l Life Insurance Co. of Canada
 - Lucent Technologies
 - Allstate Bank
 - Chevron
 - Intel
 - Hallmark
 - Shell Services International
 - Pacific Gas & Electric
- ... og hundrevis av andre, inklusive mer enn 40 universiteter og høyskoler.

nettet. Trafikken – såkalte prober, som søker etter hull og svakheter – vokste raskt i takt med at stadig nye 'sendere' av probene dukket opp. Lion-ormen angrep en kjent svakhet i navnetjenesten BIND, og infiserte på kort tid tusenvis av maskiner. Ormen samlet passord-filer fra infiserte maskiner, sendte dem til Kina, og installerte samtidig et verktøy som på kommando (via nettverket) kunne starte et såkalt *Denial of Service* angrep (DoS, se Mellvik-Rapporten nr. 73 og 82) i lokalnett og intranett. Sist, men ikke minst installerte ormen seg selv, og benyttet den nye verten som utgangspunkt for å finne og angripe flere ofre.

Hadde angrepet kommet bare noen måneder tidligere, ville all verdens innbruddsalarmer ha ringt forgjeves. De kunne fortelle at noe galt var fatt lokalt og sørge for lokal håndtering, men ikke bidra til en tidlig og samtidig alarm over hele verden, eller trigge en advarsel til titusenvis av organisasjoner som var utsatt, men fortsatt ikke angrepet. Sannsynligvis ville det tatt flere dager før nyheten var ute hos de som trengte den, mer enn nok tid til at spredningen for Lion ville ha vært total.

Denne gangen gikk det imidlertid annerledes. Sensorene sendte sine data til analyse ved de regionale sentrene. Ved ett av dem ble det registrert en økning i prober på port 53 fra noen hundre om dagen, til over 50.000 den 22. mars i år. En time senere hadde kvalifiserte spesialister³ analysert dataene og konkludert med at en global Internett-storm var under oppseiling. En ansvarlig aksjonsgruppe ble utpekt og forespørslers om kontrollinformasjon ble sendt til hundrevis av kontakter over hele verden: "Har dere registrert unormal trafikk av følgende typer ...?"

Tre timer senere tikket meldingen inn fra en systemadministrator i Holland, som hadde registrert infeksjon på flere maskiner. I de neste 24 timene kom tilsvarende meldinger fra Brasil, Canada, Venezuela, Storbritannia og USA.

I mellomtiden hadde ekspertgruppen tatt for seg en kopi av Lion-programmet, analysert det og utviklet et verktøy som raskt kunne fortelle om et system var infisert. FBI ble informert og 14 timer etter at de første stormkastene ble registrert, fikk 200.000 kontakter over hele verden informasjon per epost med detaljer om angrep som fortsatt var underveis, og råd med hensyn til hvordan det burde håndteres. FBI underrettet sine nasjonale og internasjonale kontakter, og Internett-leverandøren UUNET fikk stengt forbindelsen til den kinesiske mottakeren av alle passordfilene.

The proof of the pudding ...

Hendelsen demonstrerte for det første hvilken enorm verdi samarbeid over alle grenser har for å bekjempe stormer og angrep i en elektronisk verden. Dessuten – og like viktig – ble verdien av trafikk-overvåking i sann tid kvantifisert: Uten mulighet for å sammenstille tallene over

Sikkerhet og sløvhet

Det er verdt å minne om at også i tilfellet Lion var det ingen ny svakhet som ble utnyttet for å få aksess til systemene. Den hadde vært kjent – og tettet – i over et år. Det samme scenariet går igjen og igjen – nylig i forbindelse med en svakhet i Microsofts IIS: 3 måneder etter at selskapet hadde informert markedet og klargjort en 'fix' (*patch*), ble 400.000 systemer offer for innbrudd gjennom nettopp denne svakheten.

Videre demonstrerte **Code Red** viruset, som herjet i juli og fortsetter i inneværende måned, at sløvhet med hensyn til justering av klokker og datoer kan ha mer dramatiske konsekvenser enn noen hadde forestilt seg: Viruset blir styrt av klokken – det bytter modus kl. 0000 en gitt dato, slår seg av på en annen dato osv. På grunn av datofeil på tusenvis av IIS-tjenere verden over, fortsatte imidlertid angrep og spredning etter at virusets opphavsmann hadde ment at det skulle stoppe. Konsekvensen er langt større og mer langsiktige skadevirkninger.

Varsling og informasjonsspredning er med andre ord kun én av en rekke utfordringer knyttet til forbedring og opprettholdelse av sikkerhetsnivået. Ikke rart IT-sikkerhetens *Grand Old Man*, Gene Spafford, proklamerer sløvhet som sikkerhetens verste fiende (se side 29).

³ Alle analytikere som deltar i arbeidet for Internet Storm Center må være 'GIAC-sertifiserte', se side 10.

større områder, ville trafikkøkningen fra Lion ikke blitt tilstrekkelig synlig til å forårsake reaksjoner. Kun de regionale og globale sammenstillingene var tilstrekkelig avvikende til å trigge alarmen.

Fra hendelse til storm

Teknologien, ekspertene og nettverkene som oppdaget Lion-ormen var alle med i et samarbeid som ble kalt '*Consensus Incident Database*' (CID), etablert i november 2000 på initiativ fra og under styring av SANS Institute. Innsatsen og resultatene fra disse hektiske marsdagene la grunnlaget for navnet vi bruker i dag – *The Internet Storm Center*.

I dag mottar Storm-senteret over 3 millioner informasjonselementer fra kontrollsystemer (IDS, *Intrusion Detection System*) over hele verden daglig. Aktiviteten er i kraftig vekst for å raskere og mer effektivt kunne detektere hendelser og stormer av betydning, isolere områder som er angrepet, og formidle relevant informasjon og kunnskap om ormer, virus og andre angrep mot systemer og nettverk over hele kloden.

Gratis-tjenester

Dessuten – og like viktig: Tjenestene fra Internet Storm Center er gratis. De direkte kostnadene dekkes av SANS Institute.⁴ Titusenvis av kursdeltagere over hele verden genererer et betydelig overskudd i løpet av et år, som i sin helhet pløyes tilbake i aktiviteter knyttet til sikkerhet, systemadministrasjon, sponning av *Open Source Software* prosjekter og stipendier.

Utover løpende overvåking samt koordinering av informasjonsflyt og 'kommando-grupper', sørger ISC for utvikling av verktøy som tester sikkerheten på ulike plattformer. Samtidig koordineres videreutviklingen av programmene ('sensorene') som ekstraherer og samler inn den løpende informasjonen – via kontinuerlig analyse av loggfiler fra all verdens brannmurer og filtreringsprodukter: Snort, Raptor, PortSentry, BlackICE, ZoneAlarm, SonicWall, og mange flere, samt fra selve operativsystemene og fra DSL/kabel-rutere fra ulike fabrikanter.

En raskt voksende kunnskaps- og informasjons-database står sentralt i virksomheten: Her registreres hendelser, virus, nettsteder, programmer, hull, svakheter og mye mer – et elektronisk bibliotek som for det første skal være lett tilgjengelig for ekspertene som analyserer nye trusler, og dessuten gir referansemateriale for studier og opplæring. En liste på over 200.000 personer med sikkerhet som hel- eller deltids profesjon utgjør referansepunkter over hele verden, og over 100.000 system- og sikkerhetsansvarlige mottar ukentlige (eller oftere) epostmeldinger med oppdateringer om nytt på sikkerhetsfronten.⁵

4 SANS Institute (www.sans.org, SANS står for SYSTEMS ADMINISTRATION, NETWORKING AND SECURITY) ble etablert i 1989 med formål å fremme kunnskap på og bevissthet om de nevnte områdene. Organisasjonen har 100.000 betalende medlemmer og drives i stor grad av frivillige.

5 Enhver oppegående systemadministrator og sikkerhetsansvarlig bør prioritere disse bulletinene – se <http://www.sans.org/newlook/digests/SAC.htm>.

Hjelper det?

Nytteverdien av aktivitetene i *The Internet Storm Center* er allerede demonstrert. Lederen for SANS Institute, Alan Paller, forteller at tilstrømningen av frivillige – organisasjoner og enkeltpersoner som vil bidra gjennom å levere informasjon (nett-sensorer), eller på annen måte – er 'positivt behagelig'.

Aktivitetene har allerede spart tusenvis av organisasjoner over hele verden for store kostnader og problemer, men det aller viktigste poenget er at grunnlaget for et koordinert, verdensomspennende forsvarsverk omsider er på plass. Dermed kan det hevdes at situasjonen vi beskrev innledningsvis, der Crackere og virus-utklekkere kan boltre seg uhemmet, er i ferd med å bedre seg. At ISC representerer de første vakkende skritt, gjør ikke skrittene mindre viktige.

The Internet Storm Center:

For mer informasjon se
www.incidents.org eller
www.sans.org

Utover de praktiske resultatene som allerede kan påvises, er demonstrasjons- og smitte-effektene essensielle: En hel verden ser at samarbeid nytter, og tilgangen på ekspertise, penger og andre ressurser vokser. Nasjonale programmer sponset av lokale myndigheter med støtte fra eksperter i akademiske og profesjonelle miljøer, blir satt i gang – og mange bekker små blir til slutt en stor å, også i denne sammenhengen.

Kunnskap er makt

Et annet svakt punkt vi var inne på innledningsvis, er tilgangen på kunnskap og kvalifisert personale. Sikkerhet og sikring er en kostnad, en plage og generelt ulystbetont, ikke bare for alle oss som trenger bedre sikkerhet, men tydelig også hos utdannelsesinstitusjonene. Dermed er tilfanget av opplæringsprogrammer på området i beste fall utilstrekkelig, i verste fall fullstendig fraværende.

Dette er åpenbart et dårlig utgangspunkt for kampen mot datakriminalitet generelt og for å heve sikkerheten hos individuelle organisasjoner spesielt. I enkelte sammenhenger blir det sågar hevdet at den optimale løsningen på problemet er å 'konvertere' Crackerne og bruke deres kunnskap til å bygge forsvar (se kommentar på side 27). Etter vår oppfatning er dette naivt – og et bidrag til å gjøre vondt verre. For det første er det liten grunn til å tro at de 'konverterte' sjelene skal ha blitt så redelige over natten at de fortjener noen form for tillit. Like viktig er det imidlertid at de fleste av dem har liten kompetanse, og forstår lite av det de holder på med. Å tro at det skal en ekspert til for å forårsake innbrudd eller sende ut et virus i våre dager, vitner om fullstendig fraværende kontakt med virkeligheten. Like lite som det kreves innsikt for å knuse ruter eller spre flyveblader, fordres det noe annet enn tid, PC og Internett-tilgang for å bli Cracker – innbryter eller virusforfatter.

Å arbeide effektivt med innbruddsdeteksjon, sikring, filtrering og kontrolltiltak, krever en bredde og dybde av teknisk innsikt og erfaring som er vanskelig å finne under normale omstendigheter, og praktisk talt umulig å oppdrive i et stramt arbeidsmarked. Derfor tok det samme SANS Institute som står bak *Internet Storm Center*, for en tid siden initiativet til et opplærings- og sertifiseringsprogram for sikker-

hetsspesialister. Organisasjonen har allerede i mange år levert kurs, seminarer og konferanser med fokus på systemadministrasjon og sikkerhet, og har hatt god tilgang på de beste ekspertene i bransjen, både i USA og andre deler av verden. Et bedre utgangspunkt for å utarbeide et sertifiseringsprogram kan vanskelig finnes.

The Global Information Assurance Certification Program (GIAC)

I parallell med etableringen av *Internet Storm Center*, samlet SANS Institute over 200 nettverks-, system- og sikkerhets-ansvarlige fra små og store organisasjoner for å sette sammen et sertifiseringsprogram – en kravspesifikasjon om vi vil – for sikkerhets-spesialister. Siden tilgangen på relevant opplæring er mangelfull, ble det samtidig utarbeidet en samling kurser som støtter sertifiseringsprogrammet, og gjør det mulig for interesserte å skaffe seg den kunnskap som skal til for å komme gjennom nåløyet.

Dynamikk er et nøkkelord for GIAC-programmet. Målet er i bevegelse og det er nødvendig med en løpende tilpasning mellom virkelighetens utfordringer og opplæringen. Programmet – kursene og testene – er derfor under kontinuerlig utvikling, en stor, men nødvendig utfordring i seg selv. Likeledes ligger det i sakens natur at kandidater som sertifiseres det ene året, må arbeide aktivt innen sikkerhet og sikring for å opprettholde det nødvendige kunnskapsnivået. Slik er det innen de fleste områder, men knapt noen felter preges av en slik grad av dynamikk. Via oppdateringskurs kan sertifiserte eksperter sørge for å holde seg på høyde med utviklingen.

GIAC-programmet er delt i fire nivåer som bygger på hverandre:

- 1** Begynner (introduksjon) – *Information Security KickStart*
- 2** Grunnleggende – *Security Essentials*
- 3** Videregående – *Subject Area Modules*, 6 fordypningsområder, se nedenfor
- 4** Avansert – *Security Engineer*

Nivå 4 gir grunnlag for eksamen og sertifisering som 'IT Sikkerhetsingeniør', mens hver av de 6 modulene på 3. nivå gir grunnlag for individuelle eksamener:

- ✓ Brannmurer, 'kringvern' (*perimeter protection*) og VPN
- ✓ Avansert innbrudds-deteksjon (*intrusion detection*)
- ✓ Avansert innbruddshåndtering, opprydding, tetting av hull
- ✓ Sikring av Windows-systemer
- ✓ Sikring av Unix-systemer
- ✓ Kontroll/revisjon av sikkerheten i IT-systemer⁶

Hele opplæringsprogrammet blir i løpet av inneværende år tilgjengelig via Internettet – i tillegg til på SANS' regulære arrangementer rundt om i verden.

⁶ Denne modulen er ny og blir først tilgjengelig i disse dager.

Detaljer om GIAC-programmet er å finne i PDF-dokumentet på adressen <www.sans.org/giactc/GIAC_Cert_Brief.pdf>.

Sertifiseringen bygger på gjennomføring av kursene, et praktisk prosjekt (8 uker) med skriftlig rapport og eksamen – ikke ulikt programmer i regi av store leverandører som Microsoft, IBM og Cisco.

Hvorfor er GIAC viktig?

Årsaken til at vi vier GIAC-programmet oppmerksomhet er først og fremst at det er unikt i en verden som skriker etter mer kunnskap, innsikt og ikke minst innsats på IT-sikkerhets-området. Ved å gå foran med et substansielt eksempel, er det håp om at sikkerhet kan få høyere status og oppmerksomhet også i regulære utdanningsinstitusjoner og -sammenhenger.

Dette er ingen konkurranse om kandidatene, men et kappløp om å komme i posisjon før en ny bølge av Internett-basert kriminalitet, terror og/eller vandalisme setter inn. For hver ny 'duppedings' med Internett-konnektivitet som kommer på markedet, øker nedslagsfeltet og attraktiviteten for de tvilsomme elementene som lever for eller av å misbruke ressurser og teknologi.

Konklusjon

Sikkerhet er kjedelig, kostbart og lite populært. Det samme er opplæringen, tiltakene og den løpende overvåkingen. Nødvendige onder som er uunngåelige, men som like fullt behandles stemoderlig i de fleste organisasjoner. Desto viktigere og mer prisverdig er det at noen tar utfordringene på alvor. SANS Institute har vært og er en pionér på området, og legger ned en beundringsverdig innsats for å komme på offensiven i forhold til mer eller mindre ondsinnede misbrukere av nettverk og andre ressurser.

Vi har benyttet oss flittig av organisasjonens kurs og konferanser siden tidlig på 90-tallet, og tar av oss hatten for kvalitet og innhold som fortsatt savner sidestykke i verden. Å utnytte de ressursene som her stilles til disposisjon, er etter vår oppfatning en grunnleggende nødvendighet for enhver organisasjon som tar drift og sikkerhet på alvor. *The Internet Storm Center* står som en fyrlykt på et opprørt og mørkt hav som nødvendigvis fortsatt må føre til mangt et forlis – og enorme tap – i årene fremover. Å la være å benytte de tjenestene som tilbys, frie og betalbare, havner i en kategori som er langt verre enn naivitet.

Likeledes er det ingen vei utenom organisasjonens opplæringsprogram for sikkerhets- og systemansvarlige. Deler av programmet undervises på mer enn et dusin ulike steder i verden i løpet av året, blant annet i Stockholm – i tillegg til å være tilgjengelige som *on line* kurs. Kunnskap er makt – og billig forsikring. ■