

## Sikkerhet: Tid for outsourcing?

En fersk amerikansk undersøkelse utført av National Cyber Security Alliance (NCSA) avslører at 30% av alle amerikanere tror sjansen er større for å bli truffet av lynet eller vinne i lotto enn å bli utsatt for innbrudd, virus eller lignende på PCen. For aldersgruppen under 25 år øker prosenten til 40.

### Total forvirring

Realiteten er at 70% av alle PC-brukere blir offer for virus, innbrudd eller såkalt *phishing*, mens sjansen for å bli truffet av lynet (i USA) er 0,00001%. Videre har NCSA [www.staysafeonline.info] funnet ut at 91% av alle PCer er eller har vært infisert av en eller annen form for *spyware*, som uten brukerens viten sender informasjon til tredjepart.

Vi trenger ikke verken forskning eller god fantasi for å fastslå at situasjonen neppe er spesielt annerledes her hjemme.

En bedre påminnelse om hvor kort vi egentlig er kommet med hensyn til IT-sikkerhet, kunne vi ikke ønske oss. Etter mer enn 15 års innsats er vi lenger fra målet enn noen gang, ikke fordi innsatsen har vært dårlig eller mislykket, men fordi omgivelsene og truslene utvikler seg raskere enn tiltakene har vært i stand til å adressere.

De faktiske forhold leder frem til noen enkle observasjoner som bør være retningsgivende for det videre arbeidet med IT-sikkerhet generelt:

- ✓ **Kampen mot virus kan ikke føres på klientene.** Antivirusprogramvare kan per definisjon ikke beskytte mot annet enn gamle og velkjente virus, og er dessuten notoriske kilder til SPAM.<sup>8</sup> Virus kan ikke bekjempes på andre måter enn å immunisere klientene og blokkere spredningsmekanismene.
- ✓ **Windows er en umulig plattform å sikre.** Jo før denne realiteten erkjennes, desto raskere kan vi gjøre fremskritt i kampen for bedre sikkerhet. Igjen er poenget å nedprioritere klientene til fordel for beskyttelse på infrastrukturnivå – i virksomheter og i privatmarkedet.

### Phishing – elegant og effektiv svindel

PHISHING, som uttales 'FISHING', betegner metoder for å avlure intetanende brukere viktig informasjon som personnummer, kontonummer, kredittkortnummer, passord og lignende. Metodene er ofte en kombinasjon av epost og Websider, som ser ut som de kommer fra myndigheter, bank, kredittkortselskap eller lignende. Mottakeren blir gitt en mer eller mindre plausibel forklaring på hvorfor informasjonen må oppgis, og suksessraten er forbausende høy.

Det er trivielt å lage slike forfalskninger. De distribueres gjerne som epost-meldinger med tilsynelatende bona fide avsender, og gjerne med linker til forfalskede web-sider. Dermed havner de også utenfor nedslagsfeltet til vanlige antivirusverktøy.

Veksten i forekomsten av PHISHING-angrep er tilstrekkelig stor til at mekanismen spås å bli neste års store Internett-syke. Den eneste positive observasjonen som kan gjøres, er at dette i realiteten er SPAM. Gode SPAM-filtre – som blant annet benytter såkalte svartelister, kan redusere problemet vesentlig. Samtidig er det også et faktum at ISPer – både her hjemme og i mange andre land – fortsatt vegrer seg for å foreta skikkelig SPAM-filtrering, ikke minst fordi de er store SPAM-formidlere selv. Dermed er de fleste av oss henvist til å etablere vårt eget SPAM-forsvar, hvilket ikke er vanskelig, men krever tid og innsats (se Mellvik-Rapporten nr. 106, 107 og 113 – samt neste utgave).

Den mest effektive beskyttelsen er naturligvis bevisste og oppmerksomme brukere, men det er naivt å håpe på hjelp fra den kanten. Brukere flest, spesielt i privatmarkedet, har ingen forutsetning for å forstå VERKEN problemet, risikoen eller mekanismene. "Får vi et brev fra Likningskontoret, må vi jo svare ...".

8 En leverandør av antivirus-programvare gjorde oss nylig oppmerksom på at denne praksisen er forlatt av leverandørene. I og for seg en positiv nyhet, men realiteten er at millioner av antivirusprogrammer ikke er oppdaterte og dermed fortsatt er befengt med problemer som aldri burde ha vært der i utgangspunktet.

- ✓ **Beskyttelsestiltakene må konsentreres om infrastrukturen.** Det er høyst besynderlig og direkte uansvarlig at ISPer fortsatt vegrer seg for å sette i verk nødvendige tiltak for å beskytte sine kunder, seg selv og Internettet i sin alminnelighet mot SPAM, virus og annen søppel.
- ✓ **Forandring krever kontinuerlig oppfølging.** Nye tjenester, nye anvendelser og nye brukergrupper sørger for at sikkerhetstiltak som ikke følges opp kontinuerlig, blir ineffektive i løpet av uker eller måneder. Vi diskuterte dette forholdet i detalj i forrige utgave av Mellvik-Rapporten.
- ✓ **Den kunnskap og informasjon som tilflyter brukerne er tynn, misvisende og feilfokusert.** Brukere har ikke og kan ikke forventes å ha mer teknisk kunnskap om sine IT-verktoy enn de har om bilen eller alarmen hjemme. Risiko-bevissthet – av typen ‘spenn sikkerhetsbeltet’ eller ‘slå på alarmen, bruk sikkerhetslåsen’ – er viktig. Tjenester på lavere nivå skal være automatiske og synlige kun når brukeren skal informeres om en situasjon eller hendelse.

### Beskjeden fremgang

Slik kan vi fortsette, og de fleste poengene er kjente fra tidligere sammenhenger. Fremgangen er med andre ord beskjeden – og vi skal ikke

#### God sikkerhet uten brannmur?

Det høres i første omgang ut som en dårlig spøk. Så kommer det etterhvert velkjente sitatet fra sikkerhetseksperten Marcus Ranum frem i pannebrasken: “Brannmurer er en kostbar måte å forsinke nettverkstrafikken på.” Så erindrer vi at temaet mer eller mindre direkte har vært diskutert i Mellvik-Rapporten tidligere – i nr. 37 og 57 (begge utgavene er tilgjengelige via Web-biblioteket, se side 35).

Antagelsen om at IT-sikkerhet begynner med en brannmur er med andre ord ikke riktig. På den andre siden er det også et faktum at brannmurer utgjør en viktig del av de fleste sikringssystemer. Poenget i denne sammenhengen er at det ikke finnes noen naturgitt sammenheng mellom brannmurer og god IT-sikkerhet. Tvert imot har vi en rekke eksempler på det motsatte. Det er ikke bare fullt mulig, men i enkelte tilfeller optimalt å hoppe over brannmuren.

Det første spørsmålet som dukker opp etter en slik konstatering, er om det har noe for seg å vurdere muligheten. Er det ikke enklere å ta med brannmuren, og dermed ha etablert den sikkerheten den representerer? Joda, visst er det enklere, men er det sikrere? Svaret er tja – av de samme årsaker som lå til grunn for de brannmur-skeptiske observasjonene ovenfor. Amerikanske sikkerhetsekspertene har gjort en del viktige og lærerike observasjoner i den forbindelse. De mest interessante er:

- Enkelhet er den mest grunnleggende forutsetningen for å etablere god sikkerhet. Denne enkelheten gjelder både infrastruktur og regler. Alle skal forstå hva som er tillatt, hvorfor og i hvilke sammenhenger. Den motsatte varianten, definisjon av det som ikke er tillatt, blir for komplisert og umulig å vedlikeholde.

- Fravær av brannmurer representerer en utstyrmessig, ytelsesmessig og kostnadmessig forenkling.
- 100% pålitelig konfigurasjonskontroll er én av forutsetningene for å kunne hoppe over brannmuren. Slik konfigurasjonskontroll skal i tillegg til teknisk hvem-hva-hvor-informasjon, også fortelle hvem som har ansvaret, hvem som kan gjøre endringer, endringslogger og beskyttelse mot utilsiktede endringer.
- Sikkerhet uten brannmur forutsetter at hvert enkelt system i seg selv er sikkert, og at filtrering av unødig og ulovlig trafikk mellom nettverkssegmenter finnes. Dette utelukker miljøer som benytter Windows – uansett i hvilken sammenheng. Dessuten krever sikring på systemnivå betydelig egen ekspertise.

Dermed har vi utelukket minst 99 av 100 organisasjoner, og hele tankerekken kan synes unyttig. Det er den imidlertid ikke, fordi den retter søkelyset mot hva som må til for å etablere god sikkerhet, uansett om brannmuren finnes eller ikke:

- Dersom mer enn 50% av innsats og midler brukes på brannmurer, er sjansen stor for at vi har både dårlig og kostbar sikkerhet.
- Både brannmurer og andre sikringstiltak er bortkastet med mindre vi har en klar oppfatning av hva vi beskytter mot og hva som skal beskyttes.
- Sikring av mobile og eksterne klienter er et kapittel for seg og må behandles deretter.

MORALEN ER MED ANDRE ORD IKKE Å HOPPE OVER BRANNMUREN, MEN Å HUSKE AT EN BRANNMUR IKKE ER DET SAMME SOM GOD SIKKERHET.

reflektere lenge over essensen i punktene ovenfor for å se hvor skoen egentlig trykker: Kompetanse og forståelse.

Markedet kan fortsette å skyldes på leverandører som ikke tar sine utfordringer på alvor, leverer for dårlige produkter eller har for liten kompetanse. Den faktiske situasjonen er imidlertid at leverandørene leverer det markedet vil ha. Hvem som 'lurer' hvem kan naturligvis diskuteres, men konsekvensen av analysen blir fortsatt den samme: Vi kan ikke alle være sikkerhetseksperter, og alle organisasjoner kan ikke ha sin egen sikkerhetsekspertise. Det er ikke uten grunn at selskaper som Securitas overtar sikringsoppgavene selv for organisasjoner der sikring er en vesentlig del av virksomheten.

### **Tid for OUTSOURCING**

Dette er ikke noe annet enn *outsourcing*, og poenget i denne sammenhengen er at organisasjoner flest bør outsource ansvaret for sikkerheten snarest. Signifikante fremskritt på området vil utebli inntil spesialister overtar ansvaret for IT- og Internett-sikkerheten og kan sørge for riktige tiltak i forhold til trusler, verdier og risiko.

En av hindringene for å få fart i denne outsourcingen er at det ikke finnes standarder for hvordan kvaliteten på IT-sikkerhet skal måles. Ei heller finnes det tilstrekkelig detaljerte krav til grunnleggende sikkerhet fra myndighetenes side. Slike krav og standarder gir markedet målestokker som må til for å kunne evaluere sikkerhetstjenesters kvalitet og kvantitet i forhold til hverandre. Lyspunktet er at om det skjer lite fra myndighetene her hjemme, gir aktivitetene rundt oss – spesielt i Storbritannia, grunnlag for optimisme. Om 5 år, i 2010, tror både analyseselskapet Yankee Group og sikkerhetseksperter Bruce Schneier at 90% av alle virksomheter vil ha outsourcet ansvaret for sikkerheten. Regler og krav fra myndighetene kan akselerere utviklingen, men sendrektighet fra den kanten vil ikke stoppe den.

## **Endeløs dynamikk**

I mellomtiden sitter de fleste av oss med sikkerhetsansvar for egen organisasjon og infrastruktur. Hvilke muligheter har vi til å akselerere utviklingen i positiv retning?

Første trinn er å stikke fingeren i jorda og erkjenne realitetene. Tiden er vår største utfordring, og sannsynligheten er stor for at en sikkerhetsansvarlig har dette som en tilleggsoppgave. Det betyr videre at uansett hvor mange bøker vi kjøper og kurs vi går på, vil tiden forhindre både oppbyggingen av tilstrekkelig kompetanse, og etablering og kontroll av sikkerheten.

For de fleste vil det være fornuftig å ta fatt på veien mot *outsourcing* først som sist: Finne eksterne partnere som kan gi starthjelp, avlaste noe av ansvaret og bidra til å heve det generelle sikkerhetsnivået. Er utfordringene store i dag, kan vi garantere at de blir enda større i morgen. Uansett organisasjon, størrelse og økonomi er det ingen som i lengden kan leve med utilstrekkelig sikkerhet. Å ikke vite er det samme som å ikke gjøre jobben, uavhengig av om tittelen er administrerende direktør, IT-sjef, driftsansvarlig eller sikkerhetsansvarlig. ■