

Hypersikring: Kostbart og ineffektivt

Hva i all verden har kjøleskapet på Internettet å gjøre? Hele ideen høres tåpelig ut – vi kan og vil handle selv, og vi kan på egen hånd avgjøre hva som mangler og hva vi trenger. I virkeligheten er det spørsmålet som er malplassert. Selvfølgelig skal kjøleskapet kobles til Internettet – sammen med de fleste andre elektriske apparater vi omgir oss med – og i første omgang de som er kritiske for vår daglige rutine.

Internett i alle rom

Årsaken er verken at manglende innhold skal rapporteres automatisk til den lokale kjøpmann eller at mor og far skal kunne surfe på nettet mens de er på kjøkkenet – via en skjerm i kjøleskapsdøren. Dette er fingerte behov som hører hjemme i en reklamesnutt eller en *science fiction* historie. Forutsetningen for at alminnelige brukere skal være interesserte i en tjeneste er at den for det første oppleves som umiddelbart nyttig, og for det andre har en pris som står i forhold til den opplevde nytteverdien.

For kjøleskapets del betyr det i første omgang at dets tekniske status – utvendig og innvendig temperatur, kompressor-effektivitet, strømforbruk og så videre – løpende rapporteres til en 'alarmsentral' hvis oppgave er å rykke ut når noe er galt. De fleste av oss reiser mer enn noen gang, og har enten opplevd eller hørt om kjøleskap og fryserer som etter en teknisk feil har stått i dager og uker fulle av kostbar, råttent og illeluktende mat. Den dagen det er enkelt å forsikre seg mot at slikt skjer, er det ingen tvil om at kjølerommet, kjøleskapet, fryseren, ventilasjonsanlegget og mer til kommer på nett.

Vi trenger imidlertid ikke å gå så langt for å finne eksempler. Allerede i dag har vi stor nytte av at CD-spillere og DVD-spillere er på nett: Titler, innholdslistor og annen informasjon hentes automatisk idet vi starter en CD, og blir vist på display-anordninger som blir stadig mer allsidige. Det er lett å se for seg hvordan neste trinn i utviklingen vil eliminere både CD- og DVD-samlinger, mens innholdet i stedet blir levert over nettet når vi måtte ønske det, med den kvalitet vi foretrekker og til en pris vi finner akseptabel.¹

Jo lenger vi lar tankene fly, desto flere attraktive scenarier finner vi. Enkelte av dem blir sågar så innlysende at vi undrer oss over hvorfor de ikke finnes allerede. Samtidig øyner vi både tekniske og praktiske utfordringer som må overvinnes før slik konnektivitet og tilhørende tjenester blir en selvfølge. Hva med sikkerheten for eksempel? Alle vet og mange har erfart hvor farlig verden der ute er, og å slippe uvedkommende inn i våre elektriske apparater, fører oss raskt tilbake til *science*

¹ Vi kommer tilbake til konvergens mellom data og musikkanlegg i neste utgave.

Sikkerhet og misforståelser

fiction filmenes fryktinngytende verden. Nei, det er nok tryggest å la alt bli ved det gamle. Da har vi i alle fall forutsetning for å forstå hvordan tingene fungerer.

Vegring mot forandring er en del av vår natur. Nylig avdøde Kjell Aukrusts Ludvig-figur tar den norske folkesjela på kornet i så hen-seende. Uten en samling Solan'er blant oss – og stort press utenfra, ville det ha vært langt mellom fremskrittene 'mellom bakkar og berg'. Og kombinasjonen Internett og sikkerhet skaper lett assosiasjoner til gode, gamle Ludvig: "Det er fa'li', det!"

Men hvor farlig er det egentlig? Vel er det positivt at IT-sikkerhet gene-relt og sikkerhet knyttet til Internettet spesielt omsider har kommet på alles agenda, men problemene har lett for å få proporsjoner som full-stendig mangler forankring i virkeligheten. Løsningene blir deretter: De kurerer symptomer mens de egentlige problemene lever ufortrødent videre.

Slik blir det gjerne når alle roper ulv, mens få eller ingen har sett den. Opportunistene strømmer til for å selge oss våpen og forsvarsverker som skal beskytte og forsvare oss mot den overhengende, men akk så vage trusselen. Det er positivt at truslene tas på alvor, men når de ikke er forstått, er det bortimot umulig å bygge effektive forsvarsverker.

For mye og for lite

Ved inngangen til 2003 står vi overfor den paradoksale situasjon at vi har for mye sikring og for lite sikkerhet – nettopp fordi truslene gene-relt er lite forstått og produktene som selges, langt fra alltid angriper riktig problem.² I motsetning til den generelle oppfatningen i marke-det, er sikring noe det virkelig kan bli for mye av: Mislykket sikringsar-beid og malplasserte sikringstiltak skaper falsk trygghet, mens overdreven sikring i forhold til trusler og/eller verdi hemmer brukerne, reduserer produktiviteten og stimulerer til overlagt omgåelse av tilta-kene.

Sikkerhetseksperter Peter Tippett, grunnlegger og leder av selskapet TruSecure, holdt foredrag i Oslo i oktober 2002,³ og påpekte en rekke slike feilfokuseringer. For eksempel har det i 10 år hersket nærmest hysteri rundt bruken av kredittkort på nettet, som blir oppfattet som særdeles risikabelt med mindre datakanalen er kryptert. Mens slik kryptering i dag er normalt, er det også et faktum at det ikke finnes ett eneste eksempel på at kredittkortnummer er blitt stjålet *in transit*. På den andre siden er listen lang over kredittkort-nummere som er kom-met på avveie og blitt misbrukt etter innbrudd i leverandørens kunde-databaser.

2 Situasjonen har vært under utvikling i lang tid, se for eksempel artikkelen "Brannmurer: Mye penger, lite sikkerhet" i Mellvik-Rapporten nr 57.

3 I regi av det norske sikkerhetsselskapet Mnemonic as – www.mnemonic.no.

Eksemplet er interessant fordi enorme ressurser i løpet av perioden er brukt på krypteringsmekanismer og sikring av transaksjoner, mens systemer og innholdskontroll ved lokale inn/utpasseringspunkter har fått vesentlig mindre oppmerksomhet. Videre har tiltakene på lokalplanet typisk vært rettet mot symptomer i stedet for å angripe de egentlige problemene.

Et annet og like alarmerende forhold er følgende: Vi overflommes av sikkerhetsbulletiner, virusalarmer og rapporter om allverdens feil, svakheter og hull, og glemmer at det er risiko, ikke sårbarhet som er viktigst for god sikkerhet. Det enorme støynivået fører til at vi mister skogen av syne for trær, og konsentrerer oss om å tette små og store hull som i praksis representerer en helt forsvinnende risiko.⁴

Hvor vanskelig kan det være å få fornuften på banen? Vi har alle et forhold til sikkerhet i det daglige, til dører, vinduer, alarmer og låser. Med mindre vi har helt spesielle ting som skal beskyttes, begrenser vi oss til å stenge vinduer og låse ytterdører, mens interne dører står åpne. At en eventuell inntrenger ville få en vanskeligere oppgave dersom alle mulige dører ble stengt er innlysende, men komplikasjonene er for store i forhold til sjansene for innbrudd og verdiene som skal sikres. Sikringstiltak som er til alvorlig hinder for alminnelig anvendelse, er sjelden nødvendige og enda sjeldnere effektive.

Sårbarhet kontra risiko

Som mennesker er vi sårbare for utallige trusler i våre omgivelser. Likevel tar vi sjansen på å bevege oss utendørs, i trafikken, gå på fortau, spise mat full av e'er og andre tilsetninger og så videre. Vi beskytter oss der vi anser risikoen for å være betydelig, ulempene rimelige og kostnadene akseptable – med sikkerhetsbelter, kollisjonsputer, sykkelhjelmer, knebeskyttere og vernesko, og lar resten av sårbarheten være.

På IT-siden gjør vi det motsatte: Vi konsentrerer oss om trusler og sårbarhet, og glemmer at det er risiko som teller. I 2001 ble det oppdaget 2437 sårbarheter (hull, feil og andre mangler) i ulike utgaver av Windows, mens mindre enn 1% av dem noen gang ble registrert utnyttet av inntrengere. I 2002 var spriket enda større. En hel verden halser fra sårbarhet til sårbarhet, godt støttet av ivrige leverandører som lever av å krisemaksimere bagateller. Er det rart sikkerhetstiltakene er kostbare og lite effektive?

Feilfokuseringen har vært med oss i årevis, og har hatt en lang rekke interessante bivirkninger. For eksempel har Microsofts programvare generelt og ulike inkarnasjoner av Windows spesielt fått så hatten passer for sin manglende sikkerhet. Selskapet har svart med å introdusere sikkerhetsfunksjoner over en lav sko – først i Windows 2000, så i XP og nå i de kommende .NET-systemene. Kritikken har vært berettiget, men feilfokuseret: Det er kvalitet og design i systemene som har vært mangelfull – og fortsatt er det. Sikkerhetstiltakene som er intro-

⁴ Se også kommentar til Microsofts endrede rapporteringssystem for feil og hull på side 24.

duisert, har utvidet systemenes anvendelsesområde, og samtidig forsterket manglene, ikke redusert dem.

Det er vel og bra at vi i dag kan bruke et W2k-system som brannmur og VPN-klient eller -tjener, men dette er ny funksjonalitet, ikke redusert sårbarhet. At feil kontinuerlig blir rettet reduserer den teoretiske sårbarheten, men berører i beskjedne grad risikoen, som først og fremst er knyttet til hvor og hvordan systemene benyttes. Den grunnleggende kortslutningen er at slike systemer aldri bør eksponeres for åpne nettverk, men befinne seg bak et forsvarsverk som er tilpasset oppgaven. Tilsvarende gjelder for andre generelle operativsystemer, med mindre de har gjennomgått spesielle tilpasninger som gjør dem egnet for ruter- og/eller brannmur-oppgaver.

Over på riktig spor

Situasjonen kan ikke unngå å få konsekvenser for hvordan vi håndterer IT-sikkerhet i årene fremover. Vi kan ikke og ønsker ikke å låse alle husets dører til stadighet. Likeledes er det en praktisk umulighet å sikre hver eneste av én milliard enheter som vil være tilknyttet Internettet i 2005.⁵ Det er på mange måter et paradoks at vi må over på et mer tradisjonelt spor, der vi konsentrerer innsatsen om sikring av grensene, ikke hver enkelt innbygger, vi sikrer dørene og ikke hver enkelt verdigjenstand. Når logikken ligger på bordet, ser det unektelig merkelig ut at vi har forsøkt oss på noe annet i årevis.

Her kommer vårt innledende eksempel med kjøleskapet på Internettet til nytte: Det er klart vi er opptatt av sikkerheten når all verdens duppedingser havner på nettverket, men vi forstår at sikkerheten må etableres rundt objektene, ikke bygges inn i dem. Kjøleskap og ventilasjonsanlegg skal ikke være innbruddssikret, men utrustet med programvare av god kvalitet som utfører sine oppgaver pålitelig, og ikke har åpninger for all verdens tilleggsfunksjoner som vi aldri får bruk for. Enkelhet gir grunnlag for god sikkerhet – som sågar kan dokumenteres. Hovedpoenget er altså at det ikke er kjøleskapet eller fjernsynet som skal sikres, men inngangsdøren og huset. Inngangene skal være utrustet med nødvendige blokkeringer, kontroller, filtre og så videre. 'Boksene' som gjør denne jobben, skal være tilknyttet vårt alarmselskap som har ekspertise, ansvar og kontroll med at sikkerheten er tilfredsstillende, og til å rykke ut når alarmen går.

Helheten kontra individene

Analogien med skogen og trærne er til god hjelp for å holde fokus der det skal være – på helheten. Det er ikke viktig å tette alle mulige hull, men å sørge for at brannmur og filtrering fungerer. Likeledes er det ikke kritisk å ha verdens beste brannmur, men en brannmur som virker og er tilpasset behovene med hensyn til kapasitet og egenskaper. Videre er det av beskjedne verdi å sikre noe som helst dersom bru-

⁵ På sitt foredrag ved Consumer Electronics Show i Las Vegas i begynnelsen av januar i år, estimerte Real Networks' Rob Glaser dagens antall til ca. 300 millioner og til over én milliard ved midten av tiåret.



Toshibas kombinerte brannmur, aksesspunkt, ruter, svitsj og epost/web-filter er laget for privat- og småbedriftsmarkedet, og bidrar til å flytte fokus over fra systemer til nettverk. Produktgruppen – som omfatter over 2 dusin produkter fra omtrent like mange leverandører, er kritisk for å heve sikkerheten til et rimelig nivå, ikke minst i privatmarkedet. Alternativt kan internett-leverandørene tilby samme funksjonalitet, men interessant nok er tilbudene fra den kanten i beste fall magre.

kerne ikke har forstått vitsen med tiltakene. All verdens mekanismer stopper ikke en autorisert bruker fra å brenne en CD og ta med seg arvesølvet på innerlommen. Likeledes skal det lite teknisk innsikt til for å sette opp et ubeskyttet og 'uautorisert' trådløst aksesspunkt på kontoret.⁶ Hvor mange driftsorganisasjoner eller sikkerhetsansvarlige har levnet brukerne og opplæringen en tanke mens sårbarhetsrapportene har strømmet på de siste årene?

For IT-sikkerheten betyr fokus på helheten at vi i første omgang glemmer klienter og tjenere. Deres individuelle sikkerhetsnivå er ikke uviktig, men noe vi etablerer og justerer under installasjonen og i forbindelse med vesentlige oppgraderinger. I stedet skal vi bruke tid på fysisk sikkerhet, sikring av 'portene' mot omverden, av nettverket – og av organisasjonen gjennom etablering av forståelse og holdningsskape

pende tiltak. Når vi sier 'glemme klientene' gjelder dette også spesielle sikkerhetstiltak som antivirus-programmer og lokal pakkefiltrering. Slike tiltak er kostbare, tid- og ressurskrevende, og gir en falsk følelse av sikkerhet. Funksjonene de utfører skal gjøres på nettverksnivå, hvilket både er langt mer effektivt, billigere og vesentlig sikrere. Argumentasjonen gjelder også for hjemmekontorer, som bør være satt opp med en ruter/brannmur-kombinasjon som kan foreta innholdsfiltrering.

Denne omfokuseringen betyr ikke at dybdeforsvar er uviktig, men at det stopper før vi kommer til enkeltsystemene. Det kan riktignok argumenteres for at den totale sikkerheten blir enda bedre dersom også enkeltindividene sikres. Poenget er imidlertid at det ikke finnes ressurser nok til å sørge for god sikkerhet på individ-nivå, og at innsatsen derfor er bortkastet og totalt sett gir dårligere sikkerhet i stedet for bedre.

Fra tanke til handling

Siden perfekt sikkerhet ikke finnes og ubegrensede ressurser ikke er tilgjengelige, er god sikkerhet først og fremst et spørsmål om prioritering. En velprøvd og stadig like pålitelig metode for å få frem riktige valg i en slik sammenheng, er å spørre hva vi ville gjort dersom vi kunne sette i verk kun ett eneste tiltak! Antallet kan eventuelt økes til 2, 4 eller 6 hvis ressursene tillater det, og forholdene forøvrig ligger til rette. Med sunn fornuft og god innsikt vil de tiltakene som har størst praktisk effekt, bli valgt. Dersom tetting av hull og oppdateringer av programvare kommer med på en slik kort-liste, har vi enten ekstremt god sikkerhet allerede – eller misforstått oppgaven.

⁶ Se artikkelen "Er din organisasjon sikkerhetsbevisst" i Mellvik-Rapporten nr. 78 og "Informasjonssikkerhet: På kanten av stupet" i nr. 74.

Igjen er det nyttig å minne om at det er risikoen som skal reduseres. Risiko er på sin side sammensatt av tre elementer: Trussel, sårbarhet og hyppighet – et forhold som kan formuleres slik:

$$\text{risiko} = \text{trussel} * \text{sårbarhet} * \text{hyppighet}$$

Formuleringen er nyttig fordi den forteller at hvis én av faktorene er borte (0), er risikoen også null. For eksempel: Microsofts IIS har vist seg å være særdeles sårbar. Dersom vi ikke kjører IIS, er risikoen åpenbart fraværende. Eller: Portscanning er en trussel, men dersom vi har stengt alle inngående porter og kun tillater utgående trafikk, er sårbarheten fraværende og risikoen null.

Videre kan følgende observasjoner bidra til optimale prioriteringer:

- ✓ Viktigheten av generell trafikk-kryptering er overvurdert. VPN-forbindelser er nyttige, men først og fremst for pålitelig autentisering. Dagens VPN-produkter er kompliserte, ressurskrevende og kostbare i forhold til nytteverdien. Derfor vil SSL sakte, men sikkert overta som foretrukket transportsikring.⁷ Kryptering av intern trafikk er sjelden nyttig i forhold til kostnaden.
- ✓ Passord i klartekst skal aldri forekomme – på nett, i hukommelse, på skjermen eller på masselager.
- ✓ Gode brukerplassord er viktige, men det er enda viktigere at passordene er utformet slik at de huskes, og ikke skrives på lapper eller lagres i automatiske påloggingslister – inntil vi kommer til det punkt at en fingerscanner eller lignende overtar oppgaven.
- ✓ Innholdskontroll er viktig, og løpende oppdatering av virus-signaturer er nødvendig, men oppgaven hører hjemme ved inngangen til nettverket, ikke på den enkelte maskin.
- ✓ Tenk først, agér siden. Bruk risiko-ligningen ovenfor som kontroll: Det spiller ingen rolle hvor stor en trussel er, dersom den aldri forekommer. Et usikret system representerer ingen risiko dersom det ikke er eksponert. Og så videre.

Konklusjon

Målsettingen er ikke å etablere verdens beste sikkerhet, men tilfredsstillende sikkerhet – ut fra behov, verdier og tilgjengelige ressurser. At ressursene er utilstrekkelige er ingen unnskyldning for ikke å disponere dem optimalt. Det er utrolig hvor langt vi kan komme med erfaring og en solid porsjon sunn fornuft. Som vi har understreket flere ganger allerede, betyr det å finne hvor skoen trykker, hvorfor det trykker, hvor hardt det trykker – og først da anviser optimale tiltak. Som Peter Tippett uttrykte det: *“If you cannot think of at least 20 factors that affect a certain problem in your organization, you are not thinking.”*

⁷ Se Mellvik-Rapporten nr. 98 side 29.