

IT-revyen

Mellvik-Rapporten er verken avis eller nyhetsmagasin, men vi er definitivt opp-tatt av det som skjer rundt oss. Under overskriften IT-revyen kommenterer vi aktuelle nyheter og temaer i markedet og bransjen forøvrig. Vi konsentrerer oss om emner og trender som faller inn under MRS naturlige fagfelt, og inviterer leserne til å komme med innspill.

Hackere som beskyttelse?

Sikkerhet er blant våre primære interesser og fokusområder, ikke minst i denne utgaven. Derfor leser vi med spesielt stor interesse om et nystartet sikkerhets-selskap som med ekspertise fra et 20-talls hackere skal levere sikring til IT-Norge. "Det er kun hackere som kan beskytte oss mot sine likemenn, ingen andre har ekspertisen", hevder initiativtakeren til selskapet. Ved første øye-(eller øre-) kast kan dette virke tilforlatelig, men vent litt – dette skurrer. Og jo mer vi tenker på det, desto mer skurrer det: Sikring gir sikkerhet, som i sin tur gir trygghet. Trygghet er det vi er ute etter – trygghet for at alt er under kontroll, godt nok sikret og ivaretatt av noen vi kan stole på. Påstanden om at hackere er de eneste som er kvalifisert til å gjøre jobben er like tåpelig som å si at kun forbrytere kan være vektere hos Securitas – eller spanere i politiet. Første og siste punkt på programmet for god sikkerhet er tillit. Derfor finnes det noe som heter vandell, og som får altfor liten oppmerksomhet i våre dager. Likevel har de fleste av oss den oppfatning at forbrytere ikke er til å stole på, og derfor ikke vårt valg når oppgaver knyttet til sikring står på tapetet.

Hva er årsaken til at vi skal tenke annerledes i forbindelse med IT-sikkerhet? "Ingen andre er kvalifisert til oppgaven" – for noe sludder: For det første er hacking det samme som innbrudd. Om intensjonene er å stjele eller bare å bryte seg inn spiller ingen rolle – et innbrudd er en forgripelse på andres eiendom og rettigheter som bør forfølges og straffes. Handlingen er i seg selv diskvalifiserende for et ansettelsesforhold og andre former for profesjonell kontakt.

For det andre er det en myte at hackere er spesielt dyktige. De aller fleste av dem har minimal forståelse for hva de driver med. I forbindelse med en lang rekke pågripelser i slike saker er det avslørt at de mangler innsikt i såvel handling som teknologi, men ser på aktivitetene som 'tøffe' – i samme kategori som hærverk og tagging. Sikkerhet og sikring er et fjernt begrep og teknologisk innsikt mangelvare. De finner sine verktøy på Internettet og bruker dem i henhold til oppskriften. Gode verktøy – i mange tilfeller det samme som vi selv benytter når vi skal bygge og kontrollere IT-sikkerheten, kombinert med notorisk slapp sikkerhet, er årsakene til at de kan lykkes med sin minimale innsikt.

Hackere besitter én eneste ressurs som er mangelvare hos oss med ansvar for sikkerhet og sikring: Tid. Denne kan dessverre ikke kjøpes.

Ideen har vært prøvd tidligere, blant annet ved flere anledninger i USA. Den har aldri vært vellykket. De fleste av oss foretrekker å holde innbrytere utenfor organisasjonen. Det er krevende nok å holde dem der. Å slippe dem innenfor blir kort og godt for naivt. Vi snakker om sikkerhet, ikke veldedighet.

Selv mord for Microsoft?

Kan det være mulig? At verdens største og mest vellykkede programvareselskap er i ferd med å begå selvmord? All fornuft forteller at svaret er nei – og at spørsmålet er hinsides. Microsoft har klart seg forbausende bra gjennom den ene stormen etter den andre, og kommet ut på den andre siden om ikke uten skrammer, så i alle fall med ryggen rak, pengebingen hel – og arrogansen intakt. Dessverre. Og det er nettopp arrogansen som ser ut til å være selskapets største trussel for fremtiden. De er nå så dominante i markedet, og har – i alle fall midlertidig ristet av seg trykket fra monopol-rettssakene, at både fornuft, hemninger og selverkjennelse synes forduftet. Det nye mottoet er “Microsoft eller ingen ting”, en lett omskrevet variant av “hvis det ikke er fra Microsoft er det ikke verdt å ha”.

I og for seg en ambisiøs og aggressiv holdning – om den hadde kommet fra en noe mindre aktør. Fra Microsoft virker det annerledes – ikke bare på grunn av selskapets størrelse og dominerende markedsposisjon, men på grunn av historien: Det finnes ingen grunn til å tro at selskapet har noe annet enn sitt eget beste i tankene – helt naturlig, rent bortsett fra at markedsføringen vil ha det til at nettopp veldedige tanker er dominante: “Vi tar vare på brukernes interesser” og “vi gjør livet enklere for DEG”, heter det – blant annet i forbindelse med Hailstorm og Passport, som skapte voldsomme tumulter for noen måneder siden. Microsoft helte olje på vannet ved å forandre markedsføringen, men ikke produktene og planene. Det samme skjedde med lisensieringen av applikasjoner, som sluttet å virke for brukere som ikke oppgraderte og betalte på nytt: Microsoft trekker metoden tilbake, men forandrer ikke betingelsene og kommer tilbake ad omveier.

Slik kan vi fortsette: I løpet av sommeren har mer enn ett dusin tilfeller som peker i samme retningen, dukket opp – de fleste av dem knyttet til Windows XP: Java droppes fra XP, XP blir forsinket, SmartTags blir trukket tilbake – er noen få eksempler. Videre vekker Linux og Open Source voksende bekymring hos giganten, som har brukt mye ressurser på å forklare markedet hvilke destruktive krefter som ligger under, og deres forferdelige konsekvenser.

Markedet og domstolene har akseptert selskapets integrasjon av nettleseren i operativsystemet, og Microsoft er klar for neste runde – som trekker brukerne enda lenger inn under selskapets kontroll. Den gjennomsnittlige bruker enser ikke dette – og ser heller ikke hva som skjer, før regningen kommer på døra, eller personlige opplysninger kommer på vidvanke. Da kan det være for sent. Imidlertid finnes det både presse, myndigheter og konkurrenter som ser tegningen på veggen. Dessuten – og i praksis vel så viktig: Microsoft har selv problemer med å få både systemer og historier til å henge sammen.

Hva har så dette med selvmord å gjøre? Vi er alle i varierende grad avhengige av Microsoft-produkter for å få hverdagen til å fungere, og ønsker oss en leve- randør som tar ansvaret på alvor: I stedet for å øke kontroll og dominans, burde Microsoft konsentrere seg om å heve produktkvaliteten. Noen bedre måte å sikre posisjonen i markedet på, finnes ikke. I stedet går selskapet motsatt vei: Kvaliteten faller, mens nye mekanismer, tettere integrasjon, større kompleksitet,

høyere priser og misvisende markedsføring får voksende oppmerksomhet. Markedet og Microsoft er kort sagt på kollisjonskurs. Selvdestruksjon er neppe målet, men kan lett bli konsekvensen. Det tjener ingen av oss på – og slett ikke Microsoft.

Sverige i forkant

Mens norske politikere og fagmiljøer krangler om hvem som skal gjøre hva for å bringe landet inn i en fremtid der bredbåndskommunikasjon er like viktig som veier var i forrige århundre, demonstrerer andre land handlekraft. Eksempelene er tallrike – vi har nevnt flere av dem ved tidligere anledninger, og skal ikke lenger enn til Sverige og Finland for å finne gode eksempler til etterfølgelse¹². Ett av dem er en 64-siders rapport som nylig ble utgitt av den svenske IT-kommisjonen (THE SWEDISH ICT COMMISSION), med tittelen GENERAL GUIDE TO A FUTURE-PROOF IT INFRASTRUCTURE. Rapporten er ett av en rekke elementer i en strategi lagt i 1999, som skal gi fiberforbindelse til alle svenske hjem innen 2005. Ambisjonsnivået er høyt, men realistisk, og programmet – der regjeringen er drivkraft og kommunale myndigheter i stor grad er utførende ledd sammen med næringslivet – har fått stor internasjonal oppmerksomhet.

Etter å ha skummet gjennom denne rapporten (<http://www.itkommissjonen.se/extra/document/?id=347>), deler vi svenskenes optimisme for fremtiden: Dette er grundig, realistisk og matnyttig. Samtidig kommer vår hjemlige farse i et enda dårligere lys. Et supperåd av substansløse pratmakere – i regjeringskontorer, partiapparater, IKT-Norge og næringslivet, bruker all tilgjengelig tid på å skaffe seg oppmerksomhet i stedet for å fokusere på handling. Mon tro om vi fortsatt diskuterer hvem som bør gjøre hva når svenskene tenker seg rundt sin nye infrastruktur – klare for fremtiden – i 2005?

Sløvhet: Sikkerhetens verste fiende

Enkelte ting kan ikke gjentas for ofte. Jo viktigere, desto oftere. Her i Mellvik-Rapporten har vi terpet på ulike aspekter ved sikkerhet og sikring i år ut og år inn – med gode resultater. Riktignok er det fortsatt et stykke frem til vi kan proklamere at sikkerhet har fått den plass temaet fortjener i IT-hverdagen, men fremskrittene er markante og synlige.

Vi er heldigvis ikke alene. I USA har det i løpet av de siste ti årene dukket opp en rekke instanser og organisasjoner som tar ansvar for ulike deler av sikkerhets- og sikringsarbeidet (et godt eksempel diskuteres i artikkelen på side 4). Likeledes avholdes det regelmessig godt besøkte konferanser der ekspertene setter hverandre i stevne, og der interesserte fra hele verden kan boltre seg i kurs, foredrag, workshops og diskusjoner om alt fra kryptomatematikk til virusbekjempelse og innbruddstaktikk.

¹² Et annet eksempel er Frankrike, der regjeringen nylig bevilget 10 milliarder FF som en del av et program med samme ambisjoner som Sverige. 30 mrd. FF skal til for å flytte hele landet over i bredbåndsalderen, og de offentlige kronene skal brukes til billige lån for utbyggere. En usedvanlig pragmatisk politikk for det vanligvis så sosialistiske Frankrike, og nok et eksempel å se nærmere på for våre hjemlige pratmakere.

Professor Eugene (Gene) Spafford ved Purdue-universitetet hører hjemme i aller fremste rekke blant eksperter på sikkerhet og sikring i verden (www.cerias.purdue.edu/homes/spaf). Etter å ha mottatt en utmerkelse for sin innsats ved den 23. nasjonale sikkerhets-konferansen i Baltimore for en tid siden, oppsummerte Spaf, som han gjerne kalles, en samling interessante punkter knyttet til vår fremtid på IT-sikkerhetssiden. Utover å proklamere sløvheter som sikkerhetens verste fiende, tok han frem følgende interessante punkter:

- ✘ Mange programvareleverandører anser sikkerhetsproblematikk, for eksempel virus, for å være andres problem og ansvar, og foretar seg lite eller intet for å gjøre produktene mindre utsatt.
- ✘ Programmerere og systemansvarlige får generelt for lite relevant opplæring, hvilket fører til store mengder unødige drifts- og stabilitetsproblemer. Videre fører det til liten forståelse for viktigheten av å holde systemene løpende oppdatert.
- ✘ Ledere velger systemer og programvare ut fra direkte kostnader i stedet for langsiktige driftsmessige betraktninger. Funksjonalitet tillegges større vekt enn pålitelighet.
- ✘ Sikkerhetsproblemene vil bli større før de omsider kommer under kontroll. Årsaken er den menneskelige natur: Sikkerhet er ulystbetont og vanskelig å kvantifisere, gir lite positiv oppmerksomhet og skyves derfor lett til side.
- ✘ Virusscanning er en håpløs oppgave: Det er umulig å holde signaturfilene oppdatert, selv for de profesjonelle. Sikring av personlige (hjemme-) data-maskiner via virusscanning er umulig. I løpet av et par års tid vil det dukke opp nye virus annenhver time. Hvordan skal signaturdatabasene da holdes oppdatert?

Spafford har følgende råd til alle som arbeider med teknologi, for å bringe situasjonen raskere under kontroll:

- ✘ Sikkerhetsbevissthet må inn i design av systemer – og vi som representerer markedet må forlange slike produkter. Å plastre og bandasjere systemer som mangler skikkelig design, er bortkastet tid i lengden.
- ✘ Hold leverandørene ansvarlige for produkter som svikter på grunn av feilkonstruksjon og grunnleggende mangler.
- ✘ Sørg for bedre opplæring av programmerere og driftspersonell. Sørg for at de får relevant forståelse for hvordan brukere tenker og agerer, og innsikt i virkelige i stedet for fingerte problemstillinger.
- ✘ Gjør ikke narr av 'dumme bruker-triks'. De er resultater av mislykkede brukergrensesnitt. Systemer skal være innlysende i sin funksjon, og ikke kreve IT-relatert innsikt fra brukernes side.

Eugene Spaffords betraktninger er verd ettertanke, én for én, og finnes i sin helhet på adressen www.cerias.purdue.edu/homes/spaf/ncssa.html.

I neste utgave diskuterer vi blant annet hvor sikkerhet står på prioriteringslistene hos USAs IT-ledere. Resultatene av en fersk undersøkelse er bemerkelsesverdige.

Code Red: Ingen spøk

Code Red inneholdt bugs. Viruset kunne lett ha forårsaket langt større skade. Men det finnes ingen grunn til å latterliggjøre oppmerksomheten - oppstyret om vi vil - slik enkelte journalister har gjort. Code Red eksisterer i beste velgå-

ende fortsatt. Over 400.000 maskiner ble infisert i første omgang, og nye bølger kan starte når som helst (har du sjekket om det kommer usedvanlig trafikk inn på nettverket på port 80 i det siste?¹³). Dessuten har Code Red fortalt en hel verden av Crackere at her er et åpent hull, og demonstrert en angrepsmetode som lett kan gjøres utrolig destruktiv.

Ingen andre enn leverandøren bak programmet som blir infisert, har noen interesse av å latterliggjøre trusselen: Microsoft avslører gang på gang at deres praksis og kvalitetsnivå innen programvareutvikling er sørgelig lavt, og utspillene for å bagatellisere problemer av denne typen, vitner om at selskapet fortsatt ikke tar utfordringen på alvor. At de får med seg velrenommerte nyhetstjenester som BBC og CNET News, gjør ikke situasjonen bedre.

Desto viktigere at resten av verden lager det oppstyret som skal til for å bringe oppmerksomheten til det nivå den hører hjemme: Når 400.000 av verdens kraftigste datamaskiner er infisert av et virus som når som helst kan spy ut enorme mengder støy - og lamme store deler av Internettet, er det i høyeste grad alvorlig. Når Code Red eller lignende virus dessuten kan velge å slette masselageret fullstendig på samtlige infiserte maskiner, forstår vi litt av trusselens dimensjoner.

Skikkelige rutiner og krav for programvareutvikling kan fjerne hull av denne typen. Microsoft er langt fra alene om å befinne seg på et sørgelig kvalitetsnivå i så måte, men mest utsatt og med størst ansvar som monopolist. Som magasinet PCWorld nylig (3/8/01) påpekte: "Det holder ikke med testing av produktene, det er de underliggende utviklingsstandardene som er problemet". Hva med å ta situasjonen alvorlig, Microsoft? ■

13 På vårt eget nettverk registrer vi (3/8-6/8) gjennomsnittlig 4 prober per minutt mot TCP port 80 fra vilkårlige avsenderadresser. Ingen merkbar belastning, men en indikasjon om hvor mange aktive Code Red infiserte tjenere som finnes. At problemene ikke kommer gjennom brannmuren forhindrer ikke at skanningen fortsetter - fra stadig nye adresser.