

Microsoft og sikkerhet: En umulig kombinasjon?

2 år etter at Microsofts Bill Gates og Steve Ballmer annonserte et krafttak for sikkerhet, synes situasjonen å være status quo. Om vi skal tro de nevnte herrer – og vi ser ingen grunn til noe annet – er milliarder av dollar brent av for målet, men hvor blir det av resultatene? Har selskapets produkter blitt bedre? I så fall hvilke og hvordan? Har det hele vært et spill for galleriet?

Hva var det egentlig Bill Gates lovet i sitt mye omtalte og stort oppslåtte Trustworthy Computing program, som utpekte et nytt og totalt overordnet fokusområde for selskapet? “Vi stopper all koding av Windows XP for å foreta en gjennomgripende evaluering av sikkerheten i systemet. Samtidig sender vi alle utviklere på skolebenken for å gjøre dem sikkerhetsbevisste og lære dem sikker koding”, proklamerte Gates. Noe senere kunne Ballmer fortelle at en større oppdatering av Windows 2000 ble holdt tilbake for ekstra testing – den skulle bli perfekt.

Kort tid senere kom Blaster, Nachia og et dusin andre alvorlige virus som infiserte hundretusener av gamle og nye Windows-systemer. Sikkerhetsoppdateringene har fortsatt å strømme ut, og de perfekte patchene har uteblitt. Har det skjedd noen forandring i det hele tatt?

Windows 98 overlever

Troll i ord er følelsen vi sitter igjen med etter forrige utgaves diskusjon om operativsystemer og overlevelse. Under tittelen “Operativsystemer dør aldri” påpekte vi blant annet at uansett hva leverandøren måtte finne på, fortsetter operativsystemer sitt liv mer eller mindre på egen hånd. Forholdet er naturligvis ikke ukjent for Microsoft, og er neppe årsaken til at selskapet har ombestemt seg med hensyn til støtte for Windows 98 i fremtiden. Her er det snarere hensynet til egen business som veier tungt inn, og vi er ikke i tvil om at beslutningen er optimal.

Historisk har Microsoft benyttet to ‘virkemidler’ for å få kundene over på en ny utgave av Windows – med tilhørende lisensinntekter. Den ene er ny funksjonalitet som i seg selv er tilstrekkelig fristende. Den andre er produktsupport: Når støtten (oppdateringer, feilrettelser, brukerstøtte) legges ned og/eller nye verktøy-generasjoner ikke lenger fungerer, er kundene henvist til å ta steget. Slike oppgraderinger har dessuten hatt for vane å fremtvinge skifte av hardware. Nye operativsystemer krever uten unntak mer ressurser, til tross for at de hevdes å være raskere på både det ene og det andre området.

Denne spiralen ville ha fortsatt om ikke verden hadde forandret seg. Årsaken til at Microsoft nå har snudd i døren er uten tvil konkurransesituasjonen. Selskapet ha innsett at faren for at kundene deserterer – først og fremst til Linux eller Mac – er for stor til at de kan ta sjansen på å terminere Windows 98 (og 95) enda. Dessuten signaliserer den beskjedne oppgraderingstakten til Windows XP i det profesjonelle markedet, at behovene er feilvurdert av Microsoft. Markedet er ikke primært ute etter ny funksjonalitet eller mer moderne utseende, men stabilitet og pålitelighet. Og så underlig det kan høres, er W98 vel så stabilt som XP for de fleste alminnelige anvendelser – og et langt mer egnet utgangspunkt for en ‘halvfet’ klient mot Windows Terminal Server og Citrix Metaframe.

Det handler om tillit

Vi har i utgangspunktet den holdning at Microsoft ikke farer med tullprat, og tar for gitt at forandringer virkelig har skjedd, om de er aldri så lite synlige. Det faktiske forhold er at situasjonen sett utenfra til forveksling er lik den vi hadde for 2 eller 5 år siden, om mulig verre. Riktignok finner vi en tjeneste som hjelper sluttbrukere til å sikre sine PCer på Microsofts Web-sider. Tjenesten er verdifull, men bidrar ikke til den egentlige målsettingen med Trustworthy Computing: Å sørge for sikrere produkter. Microsoft vet like godt som resten av markedet at en forutsetning for god sikkerhet er å fjerne brukeren fra ligningen. Brukere ønsker ikke og kan

ikke være sikkerhetseksperter. Dermed er konsekvensene av Trustworthy Computing initiativet i første omgang negativt: Nok en gang har store ord og fine lovnader fordampet uten synlige spor. Unntaket fra regelen er Windows 2003 Server som uten tvil er sikrere og kvalitetsmessig bedre enn sine forgjengere. Det skulle bare mangle. Dette er progresjon, ikke sensasjon, og dette er regelen, ikke unntaket – fra Microsoft eller andre leverandører. Dermed er det ikke opplagt at forbedringene kan henføres til Trustworthy Computing programmet.

Her kommer første viktige observasjon: Betyr det at markedet og pressen vil være skeptiske neste gang det kommer en plan, en strategi eller noe annet med sus over – i markedsføringsmessig forstand – fra den kanten? Neppe. Etter maksimalt 6 måneder er det hele glemt, ting har falt tilbake til sine vante spor, og verden går videre. Dersom markedet i sin alminnelighet hadde hatt bedre (mer langvarig) hukommelse, ville mangt sett annerledes ut.

Men ikke hele markedet er like sløvt. For IT-profesjonelle – driftspersonell, utviklere, IT-ledere, analytikere med flere, synker tilliten til Microsoft i kjølvannet av slike erfaringer. Dette gjelder ikke bare tillit til koblingen mellom hva som sies og gjøres. Her har de fleste leverandører sine svin på skogen, og fartstiden har lært oss å ta store ord med en klype salt. Den tiltagende tillitssvikten, som på et eller annet tidspunkt kan føre til en tillitskrise for Microsoft, har opprinnelse fra et spekter av områder. Lisenser og kostnader er én av dem, generell programvarekvalitet en annen, og skepsis til å bli sperret inne i et hjørne er en tredje. Det finnes flere, og felles for alle er at de er fundamentert i erfaring. Nettopp her ligger Microsofts største utfordring: Selskapet må vise at det er villig til å komme markedets behov i møte i handling, ikke bare i ord. Enhver observatør er i stand til å se at forandringene som er gjort de siste årene (og tidligere for den del, men mindre opplagt), primært gagnar selskapet selv, med beskjedne eller negative effekter for kundene.

“Det er markedets feil”

“Vi retter feil og bedrer sikkerheten kontinuerlig” påpeker Microsoft, og skyver ansvaret over på kundene: Når patchene og oppdateringene er gjort tilgjengelige og annonserte kan vi ikke gjøre mer. Feil, sier markedet, og viser til Slammer-viruset fra forrige årsskifte som et godt eksempel. En svakhet i Microsofts SQL Server ble angrepet med stort hell, til tross for at en patch som rettet feilen hadde vært tilgjengelig i flere måneder allerede. En databaseadministrator kommenterer situasjonen slik: “For det første har SQL-patcher vært notorisk vanskelige å installere, med langvarig driftsstans og overtidstimer som konsekvens. For det andre er klientsiden av SQL-produktet inkludert i tredjepartsprodukter uten at det nevnes noe sted – med den følge at mange kunder ikke er klar over at de er eksponert og trenger en patch. Og for det tredje er selve tjenesten (*SQL Server Resolution Service*) som ble utnyttet av Slammer, overhodet ikke nevnt i dokumentasjonen til SQL Server 7.0.”

Tilsvarende var tilfelle for Blaster-viruset som angrep DCOM-modulen i Windows i august 2003. En patch ble gjort tilgjengelig en måned tidligere, men var vanskelig eller umulig å installere på mange systemer, og katastrofen var et faktum.

Eksemplene er tallrike, hvilket også var bakgrunnen for Ballmers nevnte kommentar til forsinkelsen av en W2k-oppdatering. Altfor ofte har uttrykket "rettelse, ny feil kommer" vært en dekkende beskrivelse på oppdateringer og patcher, et solid bidrag til det svekkede tillitsforholdet som i dag er et faktum. Som vi har vært inne på i tidligere artikler (se også faktarammen på side 4 og IT-rapporten på side 21), er dette én av faktorene som i disse dager gir en merkbar 'desertering' fra Microsoft i forvaltning og private virksomheter, nasjonalt og internasjonalt.

Monokulturer og sårbarhet

Et annet element i ligningen er fokuseringen på konsekvensene av såkalte monokulturer, homogene miljøer med samme eller nært beslektede operativsystemprodukter gjennom en hel organisasjon. Mens dette ironisk nok har vært en eksplisitt målsetting i mange organisasjoner, slår det nå tilbake med ekstrem sårbarhet. Situasjonen er forutsigbar, og det har ikke manglet advarsler fra eksperthold de siste årene. Virusangrepene i 2003 hadde spesielt dramatiske konsekvenser for slike miljøer, og spådommene peker i retning av vesentlig forverring i 2004.

Forholdet har vært gjenstand for betydelig oppmerksomhet blant eksperter og i media det siste halvåret, med en foreløpig topp da en uavhengig gruppe sikkerhets-eksperter presenterte rapporten *Cybersecurity: The Cost of Monopoly* i slutten av september 2003.¹ Microsoft unngikk å kommentere rapporten direkte, utover å avvise tankegangen. En av forfatterne, Daniel Geer, hvis arbeidsgiver (@Stake) hadde Microsoft som sin største kunde, fikk sparken dagen etter at rapporten ble publisert. Geer har vært en kjent figur i IT-sikkerhetsmiljøer i 20 år, og hans avgang sier mye om hvor følsomt temaet er.

Det virkelige problemet

Det er ingen grunn til å tvile på at Microsoft virkelig ønsker å gjøre sine produkter sikrere. Ingen ser bedre enn selskapet selv hvor negativ all publisiteten rundt sikkerhetsproblemene er, og at de ikke kan unngå å påvirke markedets innstilling i lengden. Å fokusere utelukkende på sikkerhet er imidlertid en avsporing i denne sammenheng. Problemet er ikke først og fremst manglende sikkerhet, men dårlig kvalitet – på programvare, systemer, design, dokumentasjon, verktøy og så videre.

¹ Rapporten er ført i pennen av en rekke kjente navn innen IT-sikkerhet: Bruce Scheier, Daniel Geer, Rebecca Bace, Perry Metzger, Peter Gutmann, John S. Quarterman og Charles Pfleeger, og er støttet av organisasjonen Computer & Communications Industry Association. Den er å finne på <http://www.ccianet.org/papers/cyberinsecurity.pdf> og burde med sine 25 sider være interessant lesestoff for alle som har IT-sikkerhets-ansvar. Det er ikke nødvendig å være enig i konklusjonene for å kunne høste både interessante og nyttige tanker og problemstillinger.

Tøylesløs kompleksitet

Microsofts produkter er for komplekse til å kunne gjøres pålitelige eller sikre, og utviklingen går i feil retning med høy hastighet. Ifølge selskapets egne tall vokser kodebasen i Windows NT (som nå er Windows 2000, 2003 og Windows XP) med ca. 35% per år, mens tilsvarende tall for Internet Explorer er 220% per år. Programvare-eksperter beskriver kompleksiteten i programvare som proporsjonal med kvadratet av kodestørrelsen, hvilket betyr at kompleksiteten for operativsystemene vokser med nesten 80% per år og 380% for Internet Explorer. Operativsystemproduktene er allerede minst 5 ganger større (i kode) enn noen konkurrent, hvilket gir dem mellom 15 og 35 ganger flere feil – i dag. Den forholdsmessige feilraten fortsetter å øke med veksten i kompleksitet og kodebase.

Disse tallene er verken nye eller oppsiktsvekkende. Dette er kjente forhold fra forskning på programvare og utvikling gjennom flere tiår, og farene har vært påpekt overfor Microsoft utallige ganger i årenes løp. Det er derfor ingen tilfeldighet at situasjonen er blitt slik. Selskapet har selv skapt den, bevisst og overlagt, og vært klar over risikoen. Dermed blir hele øvelsen med Trustworthy Computing temmelig underlig. Riktignok kan kvaliteten på kode som skrives fra nå av og fremover, uten tvil forbedres, men burde være en selvfølge, ikke en konsekvens av et bredt publisert initiativ. Å gjøre produktene sikre er imidlertid en umulighet og å gjøre dem vesentlig sikrere er en gigantisk utfordring med konsekvenser som selskapet neppe er forberedt på å håndtere. Derfor blir Trustworthy Computing programmet først og fremst et spill for galleriet.

Hvorfor så komplisert?

Denne enorme kompleksiteten, som vi har brakt på det rene ikke kan være noe ulykkestilfelle, er tvert imot en viktig brikke i Microsofts beskyttelsesmekanismer. Visst er det sannsynlig at selskapet i forbindelse med sikkerhetsfokuseringen har skjerpet kvalitetskravene til kode som genereres. Som vi var inne på ovenfor får imidlertid tiltaket ingen konsekvenser for 'gammel kode', som for Windows' vedkommende betyr godt over 100 millioner kodelinjer.

Dessuten – og vel så viktig – fungerer kompleksiteten som innkapsling for utallige mer eller mindre hemmelige grensesnitt som benyttes av andre Microsoft-produkter, og som bidrar til at konkurrerende verktøy vanskelig kan bli like effektive og/eller elegante som selskapets egne. Grensesnittet mellom Exchange og Outlook er et godt eksempel, som blant annet refereres i rapporten om Cyberinsecurity vi nevnte ovenfor.

Denne overlagte kompleksiteten, kombinert med lang historie og tilsvarende behov for kompatibilitet bakover, blokkerer ethvert velment forsøk på å rydde opp i Windows, Internet Explorer, Office og en lang rekke andre produkter.

Konklusjon

Microsofts kamp for sikkerheten er uten tvil genuin, men håpløs. Komplexiteten vokser raskere enn noen kvalitetskontroll kan holde tritt med, og er både sikkerhetens og kvalitetens verste fiende. Når det samtidig er et faktum at denne 'fienden' også er en 'medsammensvoren', blir tegningen – og utsiktene – temmelig klare.

Derfor finnes det kun én vei ut av uføret: Å starte med blanke ark, lage design og gjøre tingene riktig fra starten av. At det er mulig, hersker det ingen tvil om. Microsofts utviklingsbudsjett på over 50 milliarder kroner årlig rekker til de største underverker på programvaresiden. Praktisk gjennomførbart er det imidlertid ikke, og politisk uakseptabelt fordi å gjøre tingene riktig i utviklingsmessig forstand, uvegerlig ville medføre en grad av åpenhet og ryddighet i grensesnittene som vil ødelegge (eller åpenbare) deler av selskapets teknologiske fundament.

En umulig oppgave

Vi kaster med andre ord bort tiden når vi streber etter å sikre produktene gjennom å installere alle tenkelige sikkerhets- og funksjonsoppdateringer. Selv for en kompetent privat-bruker er dette en uoverkommelig oppgave. Det blir som å forsøke å stoppe regnet fordi vi blir våte. En paraply er langt mer effektiv. Produktene er ikke og kan aldri bli sikre. Å sikre dem er like umulig som å stoppe en regnbyge som er i gang.

At de ikke kan sikres er imidlertid ikke det samme som at de ikke kan brukes. Systemene som kjører produktene må beskyttes, slik at deres eksponering for Internettets 'vill vest' blir minimal. Det gjelder ikke bare Windows, men også (for eksempel) IIS og Exchange – som bør unngås, men som alternativt kan gjemmes bak proxyer. Internet Explorer er en større utfordring både på grunn av sin eksponering, sine tette koblinger og dermed snarveier til operativsystemet, og ikke

minst brukerskaren. Derfor vil IE forbli Microsofts største sikkerhetsmessige hodepine i årene fremover, hvilket utgjør et kraftig incentiv til markedet for å evaluere og ta i bruk alternativer. Det er jo ikke slik at alternativene ikke finnes, men at markedet generelt er for ubevisst til å bruke dem.

Kringvern er nøkkelordet for sikring av Windows-miljøer – å sørge for at infrastrukturen er godt sikret, og eksponeringen av usikre systemer minimal. Oppdateringer skal ikke unngås, men samles opp, evalueres i forhold til miljø og behov, og installeres når det er praktisk eller av andre årsaker nødvendig. Likeledes er det positivt for både driftssik-

Paradoks?

Faktum 1: Virus og andre sikkerhetstrusler finnes fordi de har et 'marked', objekter som kan smittes og som kan bære smitten videre.

Faktum 2: Sikker programvare finnes ikke. Små programmer kan bevise å være sikre, større programmer er mindre sikre, store programmer har alltid hull.

Faktum 3: Programvare har forskjellig kvalitet – på samme måte som alle andre produkter. I motsetning til hva tilfellet normalt er for andre produkter, er programvarekvalitet imidlertid ikke proporsjonal med pris. Det må andre kriterier til for å etablere kvalitet og dermed graden av sikkerhet.

Faktum 4: Et betydelig antall programvareprodukter, fra Microsoft og en rekke andre leverandører, er kjent for å ha betydelige kvalitetsmessige og sikkerhetsmessige svakheter, mens andre produkter har motsatt renommé.

Spørsmål: Hvorfor brukes ikke de anerkjente sikreste produktene til oppgaver som er spesielt kritiske (trafikkregulering, kontroll av atomkraftverk, kontroll, styring av medisinsk utstyr og så videre)?

Det finnes eksempler på at både atomkraftverk og kraftnett er blitt satt ut av spill på grunn av virus i kontroll- eller styringssystemene.

Problemet har ikke først og fremst med programvarekvalitet og sikkerhet å gjøre, men med bevissthet og ansvarlighet.

kerhet og IT-sikkerhet å unngå stor grad av homogenisering. Å velge plattformer som er optimale for oppgaven er riktig av alle årsaker, mens å velge plattform for å homogenisere som regel er negativt.

Det er ironisk at Microsofts beslutning om å forlenge levetiden på Windows 98 og eldre, bidrar positivt til IT-sikkerheten i verden. Til tross for at disse systemene er beryktet for sin manglende sikkerhet, er de i årenes løp blitt temmelig robuste. Videre er de både enklere og mindre hullbefengt enn nyere produkter, med den åpenbare konsekvens at det finnes færre hull som kan utnyttes. Stabilitet og sikkerhet har mange fasetter.

Om Microsoft og sikkerhet er en umulig kombinasjon? Slett ikke, men for produkter hvis opprinnelse strekker seg lenger tilbake enn 12-18 måneder, mener vi at høy sikkerhet er en drøm som aldri kan realiseres. Den erkjennelsen bør få konsekvenser for hvordan vi velger, hvordan vi legger opp vår sikkerhetsstrategi, og for hvilke verktøy vi benytter. De fleste av oss er avhengige av Microsofts produkter, og må sørge for tiltak som gjør at vi både utnytter dem og samtidig får det sikkerhetsnivå vi trenger. Det er krevende, men langt fra umulig. ■