

# Microsoft og sikkerhet

*"Hvor vi kommer fra, hvor vi er og hvor vi skal"*



**Microsoft®**

## Microsoft og sikkerhet

Fakta & realitet vs media og markedets oppfatning  
Geir Hansen - Løsningsarkitekt, Microsoft Norge

Microsoft og sikkerhetsproblematikk er stadig en gjenganger i IT-presse hvor man sitter igjen med et inntrykk av at Microsoft fortsatt er en "versting" når det gjelder sikkerhethull og tilsyne-latende har gjort lite og oppnådd lite i løpet av de siste årene. Inntrykket man sitter igjen med enten man leser IT-presse eller øvrige media er at Microsoft er og blir en trussel mot IT-sikkerheten og at andre leverandører som feks. Apple, Oracle eller operativsystemer som Linux er et sikrere valg. Jeg vil i denne artikkelen redegjøre for mange av de tiltakene Microsoft har gjennomført i løpet av de siste fire årene samt klargjøre vår sikkerhetsstrategi med hensyn på hvor vi kommer fra og hvor vi skal.

### Bakgrunn

Denne historien begynner høsten 2001 med først Code Red og deretter Nimda som begge angrep svakheter i Microsofts web server og spredde seg med stor hastighet. Nettverk og servere var nede dette påførte kundene enorme kostnader. Kundene var i harnisk og det toppet seg med at analyseselskapet Gartner Group anbefalte kunder å ikke benytte Microsofts web-tjener.

Det var på dette tidspunktet at det ble tydelig at vi hadde fundamentale problemer rundt sikkerhet i våre produkter.

Hva har vi gjort over de siste 3 årene for å adressere sikkerhetsutfordringene?

Nimda og Code Red er eksempler på virus som resulterte i et ekstremt viktig initiativ eksternt og internt hos Microsoft kalt Trustworthy Computing (TwC). I januar 2002 sendte Bill Gates ut en e-post til alle ansatte som beskrev utfordringene selskapet sto overfor og hva vi måtte gjøre for å komme på rett vei. Dette var en e-post fra Bill med samme tone og viktighet som tidligere har vært sendt når selskapet har stått foran større strategiske endringer med vital betydning for selskapets fremtid. Dette resulterte i en rekke konkrete tiltak som ennå pågår og som jeg vil utdype nedenfor.



TwC brukes som et paraplybegrep for hele vår sikkerhetsstrategi og har fire hovedpillarer:

- **Visjon.** Visjonen om datasystemer like selvfølgelig, stabilt og med den kvalitet slik som vi er vant til å få fra elektrisitetsforsyningen, telefonen eller vann i springen
- **Teknologiutvikling.** Forskning og utvikling av produkter og tjenester for å realisere visjonen i TwC.
- **Sikkerhet i design, standardinstallasjon og utrulling/drift.** Endringer og forbedringer i forhold til hvordan vi i dag designer, utvikler, tester og tilgjengeliggjør våre produkter.
- **Kommunikasjon.** Endringer i hvordan Microsoft håndterer kommunikasjon rundt sikkerhetsfeil, virusangrep og sikkerhetsoppdateringer med kunder og partnere.

## Visjonen om Trustworthy Computing

IT sikkerhet er et industriproblem og dagens situasjon truer i praksis vekst og videre utvikling for hele bransjen. Visjonen om Trustworthy Computing handler om IT systemer som man kan stole på er alltid tilgjengelige, tar vare på brukerens konfidensialitet og privatliv, er sikre mot ondskinn angrep og beskytter individet mot uønsket kommunikasjon og informasjon (spam). En god analogi til dette er hvordan vi opplever en del andre tjenester som har vært tilgjengelig i mange tiår slik som elektrisitets-forsyningen, vannet i springen, telefoni og TV. For at vi skal komme dit krever det en rekke tiltak knyttet til eksisterende tjenester og systemer, men også utvikling av ny teknologi og tjenester som må være tilgjengelig i markedet. Microsoft anser seg selv, som sentral leverandør og markedsleder, å ha et særdeles stort ansvar her.

### Hvordan Microsoft designer, utvikler, tester og tilgjengeliggjør våre produkter

Da Bill Gates skrev memoet til alle ansatte om TwC resulterte dette umiddelbart i at utviklingen av neste versjon av Windows Server (som senere skulle bli Windows Server 2003) ble stoppet. Over 5000 utviklere ble sendt på opplæring i trusselmodellering og hvordan man skulle utvikle sikker programkode. "Sikker" koding i kontekst av en sammenkoblet verden var på den tiden ikke akkurat en standard del av pensum på verdens universiteter. I tillegg ble det iverksatt tiltak for gjennomføring av formell kodegranskning av alle moduler samt at en rekke konkrete designendringer ble foreslått for å redusere angrepsflate i programvaren. Vår web-tjener gjennomgikk fundamentale designendringer for å adressere sikkerhetsutfordringer som dagens design medførte.

Alle disse tiltakene ble utover våren 2002 formalisert i noe man internt hos Microsoft kaller Security Development Life Cycle (SDL) og som er blitt en del av Common Engineering Criteria (CEC), et sett med design- og prosessprinsipper som er pålagt alle produktgrupper. Windows Server og Windows XP Service Pack 2 er de første produktene hvor man ser resultatene av dette reflektert. CEC består av en rekke prosesser og krav som blir pålagt produktgruppene, men hvor spesielt sikkerhet i form av SDL har en sentral rolle. Oppsummert består sikkerhetskriteriene av følgende:

- Trusselmodellering og sikker koding. Alle komponenter eller delprogrammer skal ha en trusselmodell som beskriver flest mulige tenkelige scenarier hvor komponent benyttes til feks. å angripe andre deler av systemet eller bryte seg inn i systemet.
- Sikkerhets testing. På bakgrunn av trusselmodellen skal det også bygges test scenarier mhp sikkerhet som modulen må testes for og bestå.
- Kodegranskning. Alle moduler skal gjennom "uavhengig" kodegranskning mhp sikkerhet. Med uavhengig menes at koden skal granskes av noen andre enn de som er ansvarlig for å utvikle den.
- Prinsippet om færrest mulig privilegier. Alle moduler skal støtte prinsippet om "færrest mulig privilegier". Det vil si at modulen skal skrives og testes for så lave rettigheter som mulig og kun ha det som kreves for å utføre de oppgavene som den er satt til. Dette sikrer at det ikke skal være mulig å bruke eventuelle sikkerhethull i koden til modulen for å angripe andre deler av systemet eller utenfor systemet.
- Avslåtte standardinnstillinger. Alle funksjoner og tjenester skal som standardinnstilling være slått av og man skal måtte gjøre en bevisst handling for å aktivere dette. Hensikten med dette er å redusere mulig "angrepsflate" mest mulig for ondskinn kode. Vi ser konkrete eksempler på akkurat dette prinsippet i feks Windows Server 2003 og ikke minst i Windows XP Service Pack 2.
- Forbedring av kodeanalyse. I tillegg kreves det at all kode skal skannes og analyseres med automatiserte verktøy for å oppdage de vanligste type sikkerhets kodefeil, bla det som heter "buffer overruns".

## Tilgjengeliggjøring, utrulling og oppdatering av produkter

Alle tiltakene beskrevet ovenfor er preventivt fokusert. Det vil si, å hindre at kode som inneholder sikkerhetshull utvikles og blir en del av et tilgjengeliggjort produkt ute i markedet. Dessverre er det slik at mennesker gjør feil og programvaren som bygges i dag øker stadig i kompleksitet og volum. Vi kan med sikkerhet si at nye sikkerhetsfeil vil oppstå, både i Microsoft programvare eller i andre leverandørers programvare. Sikkerhet er et industriproblem, ikke et problem som er unikt for Microsoft, noe som også de siste ukers sikkerhetsoppdateringer fra andre leverandører og trendene i antall sikkerhetsoppdateringer viser.

Microsoft har et enormt volum av installasjoner på verdensbasis, både av kode som er skrevet før CEC ble innført, i tillegg til at det vil alltid være en mulighet for at sikkerhetsfeil også i nyere kode skal bli oppdaget også er tilstede. Vi har derfor som et av tiltakene fokusert mye på tre viktige områder:

- Oppgradere eksisterende programvare ute hos kundene til nyeste versjon. Microsoft har over de siste 3 årene jobbet intenst med å overbevise kunder om at å oppdatere til siste versjon vil gi de betydelig redusert risiko i forhold til sikkerhet. En fordel i forhold til sikkerhet er en betydelig redusert sannsynlighet for nye sikkerhetshull samt at måten programmene er laget på i mye større grad er designet for å ivareta sikkerhet i en sammenkoblet Internett-basert verden. Ofte blir våre oppgraderingsinitiativ misforstått som salgsforsøk, men for store deler av kundemassen vår dreier det seg om å oppgradere til versjoner av programvaren de allerede har kjøpt rettigheter til.
- Tilgjengeliggjøring av verktøy og programvare for enklere å kunne oppgradere og rulle ut sikkerhetsoppdateringer. Microsoft tilbyr to type løsninger her: Windows Update Services (WUS) som er tilgjengelig gratis til alle kunder og tilbyr funksjoner for automatisk å rulle ut sikkerhetsoppdateringer til Windows systemer. I tillegg har vi Systems Management Server som må lisensieres men tilbyr en rekke funksjoner utover det WUS gjør.
- Oppfordre kunder til å etablere infrastruktur, prosesser og rutiner for raskt og automatisk å kunne rulle ut og oppdatere sin maskinpark med de nyeste sikkerhetsoppdateringene. Ingen leverandør kan garantere for at deres programvare er fri for sikkerhetshull. Programvare vil også ha behov for regelmessig oppdateringer med mer generelle feilrettinger. Det spesielle med feilrettinger som tetter sikkerhetshull er at de er a) tidskritiske i tilfelle et virusangrep som utnytter hullet oppstår, og b) treffer alle brukerne i en organisasjon, ikke bare de som benytter den spesifikke applikasjonen eller funksjonen. Mao. behovet for å måtte rulle ut en sikkerhetsoppdatering i løpet av kort tid grunnet et angrep som utnytter et sikkerhetshull til et stort antall maskiner før eller siden er overveiende sannsynlig. Derfor er det svært viktig at kunder har et bevisst forhold til å etablere en infrastruktur som gjør det mulig å gjennomføre dette og regelmessig "trener" på å gjennomføre oppdateringsprosessen på tvers av en kanskje geografisk omfattende organisasjon.

## Kommunikasjon rundt sikkerhetsfeil, virusangrep og sikkerhetsoppdateringer

Det siste punktet i vår tiltaksplan gjelder hvordan vi kommuniserer med våre kunder, partnere og sluttbrukere rundt sikkerhetsfeil og oppdateringer som retter disse. Her er stikkordene tydelighet, forutsigbarhet, tilgjengelighet og timing av informasjon. I løpet av de siste årene har vi gjennomført følgende tiltak rundt akkurat dette:

- Innføring av et forutsigbart tidspunkt for når sikkerhetsbulletiner og sikkerhetsoppdateringer ble tilgjengeliggjort. Dette er den så mye omtalte patch "Patch-Tuesday" som til tider er mye omtalt i pressen. Microsoft har innført dette både for å skape forutsigbarhet på når publisering av eventuelle nye feil og rettelser kommer såvel som å legge til rette for en månedlig syklus der man "driller" oppdateringsprosessen hos større bedrifter.
- Standardisering av terminologi og klassifisering av sikkerhetsfeil. Tidligere hadde hver enkelt leverandør sin klassifisering av alvorlighetsgrad av sikkerhetshull samt at man benyttet ulike terminologier for hvordan man omtalte og beskrev disse. Resultatet for kundene våre var forvirring og usikkerhet om hvordan de skulle agere i forhold til de sikkerhetsbulletinene som ble sendt ut fra de enkelte leverandørene. Microsoft
- Kommunikasjon til sikkerhetsansvarlig ved virusutbrudd eller ved avdekking av kritiske sikkerhetshull. Tidligere var større virusutbrudd eller alvorlige sikkerhetsfeil noe man primært hørte gjennom media. For å kunne maksimere tiden kundene våre har tilgjengelig til å forberede og rulle ut sikkerhetsoppdateringer samt ta andre preventive tiltak (feks stenge tilgang til visse tjenester i nettet sitt i en periode) sørger Microsoft nå for å proaktivt enten kontakte kunden på e-post med et varsel eller at Microsoft kontakter kunden sikkerhetsansvarlig direkte per telefon gjennom sitt supportapparat.



## Resultater og status - fakta og realitet

Så hva har Microsoft oppnådd med disse tiltakene i løpet av de siste 4 årene? Har vi blitt noe sikrere? Har vi færre sikkerhetshull? Er vi fortsatt verst i klassen til sammenligning med andre leverandører?

Dette er et område som er vanskelig å måle og man vil alltid få en debatt om hva som er de rette målekriteriene. Hvis vi ser på omtale i media kan man kanskje få inntrykket av at lite har skjedd, men bildet er nok en del nyansert i forhold til dette. Selv så har vi våre interne målekriterier som vi anser som relevante mål for om vi beveger oss i riktig retning mot målet om å være en sikrere leverandør og å tilby produkter og løsninger som er med på å realisere visjonen om Trustworthy Computing. De viktigste målekriteriene vi har er først og fremst antall sikkerhetshull oppdaget per tidsenhet og alvorlighetsgrad etter en produktlansering og nttall dager det går fra et sikkerhetshull er oppdaget til Microsoft klarer å tilgjengeliggjøre en oppdatering som tetter igjen dette hullet. Figuren nedenfor illustrere den drastiske endringen i antall sikkerhetshull før og etter tiltakene ble iverksatt for henholdsvis produktene Windows Server 2003, Office 2003 og SQL Server Service Pack 3.

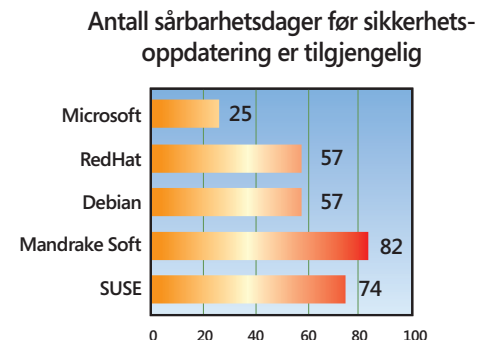
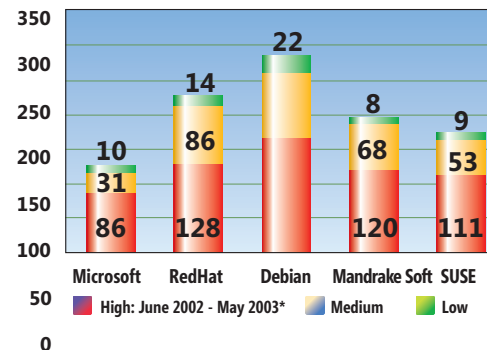
### Important + Critical bulletins issued after product release



1027 Days After Product Release

\* As of February 14, 2006

I pressen får vi inntrykk av at Microsoft har både flere sikkerhetsfeil, og at de er alvorligere enn for andre plattformer. Statistikk fra uavhengige kilder som Forrester og NIST viser noe annet. Microsoft har både lavest antall sikkerhetsfeil, lavest i henhold til alvorlighetsgrad samt færrest antall dager på å tette igjen og tilgjengeliggjøre oppdateringer til sammenligning med for eksempel de vanligste Linux-distribusjonene.



Som dataene ovenfor indikerer, ser vi en klar og tydelig trend. Hvis man anser målekriteriene ovenfor som en riktig måte å måle fremgang på er det mange ting som tyder på at vi er på rett vei. I tillegg har vi en del uavhengige og positive uttalelser fra viktige kilder som påpeker at Microsoft faktisk er på riktig vei i sin satsning:

- IDC report, Januar 2006: Microsoft Security Response Center: Taming the Chaos of Security Incidents with a Steady Process, The > <http://www.idc.com/getdoc.jsp?containerId=34810>
- ComputerWorld, 20. Januar: Microsoft Earns Patching Praise from IT Execs > <http://www.computerworld.com/securitytopics/security/holes/story/0,10801,107938,00.html>
- Microsoft Windows Platform Products Awarded Common Criteria EAL 4 Certification: > <http://www.microsoft.com/presspass/press/2005/dec05/12-14CommonCriteriaPR.mspx>
- Forrester Research, August 2005: Limited Worm Impact Shows That Microsoft's Security Strategy Is Working > <http://www.forrester.com/go?docid=37588>
- Forrester Research, March 2004, Is Linux More Secure Than Windows?: > <http://www.forrester.com/go?docid=33941>
- Gartner Group, 24. November 2004: IIS Is No Longer the Problem in Web Server Security > [http://www.gartner.com/DisplayDocument?ref=g\\_search&id=462153](http://www.gartner.com/DisplayDocument?ref=g_search&id=462153)

### Veien videre

Dette sett i sammenheng med de tiltak som er gjennomført er oppløftende, men gir samtidig ingen grunn for oss til å hvile eller føle oss beroliget. Microsoft er og vil fortsette å være spesielt utsatt som mål for ondssinnet kode gitt våre markedsandeler. Enhver leverandør med betydelige markedsandeler vil være det. Dette gir oss også et ekstra stort ansvar overfor våre kunder og sluttbrukere som vi er svært bevisst. Vi må fortsette å gjøre det vi gjør, enda bedre. Vi må fortsette å forbedre utviklingsprosessen vår for å forhindre at det skrives og tilgjengeliggjøres kode med sikkerhetsfeil. Vi vet også at mennesker gjør feil, og at sikkerhetsfeil også vil bli oppdaget i fremtiden. Derfor må vi fortsette å utvikle og forbedre verktøy for å automatisk kunne oppdatere eksisterende installasjoner og utdanne og hjelpe våre kunder med hvordan de skal sørge for at de har en beredskap og etablerte rutiner i forhold til å oppdatere installasjonene sine med sikkerhetsoppdateringer.

Sist, men ikke minst, så har vi et ansvar for å fortsette å drive utviklingen fremover med produkter å tjenester som videre understøtter visjonen om IT systemer like selvfølgelig tilgjengelige, til å stole på og sikre som annen infrastruktur som i dag er en integrert del av vår hverdag som elektrisitet, vannforsyning og telefoni. Microsoft er seg dette bevisst og jobber hver dag for å realisere dette.

Ønsker du å vite mer besøk Microsoft sin web på <http://www.microsoft.no/sikkerhet>

***Microsoft***<sup>®</sup>

Ønsker du å vite mer, besøk Microsoft  
sin web på: [www.microsoft.no/sikkerhet](http://www.microsoft.no/sikkerhet)