

Brukere under lås og slå

Tenk deg at du kjøper ny bil – en spennig og velutrustet variant som er godt egnet til såvel formålet som til å imponere naboen. Bilen blir levert, og det første du gjør er å sveise igjen bagasjerom og alle unn-tatt én dør, fjerne dekkene og pedalene, dekke vinduene og installere turtallssperre. Så er doningen klar til bruk.

Naturstridig vanvidd

Glade vanvidd? Naturligvis – men like fullt en god beskrivelse av hvordan alminnelige kontor-PCer bør håndteres. Og akkurat dette er hva som gjøres – i raskt voksende antall organisasjoner. I USA passerer tallet i disse dager 40% av alle virksomheter,⁴ og utsiktene for verktøy-leverandører som har spesialisert seg i segmentet er gode. Det beskri-vende faguttrykket er 'PC-lockdown', som burde vært en spøk, men er en nødvendighet for de aller fleste PC-miljøer.

Drift og sikkerhet tatt på alvor

Selv Motsigelsen har sin opprinnelse i en situasjon de aller fleste av oss kjenner altfor godt: Ustyrlige PCer og uløselige driftsproblemer. I likhet med PCer anno 1982 er dagens PCer laget for å klare seg selv, være selvstendige. I motsetning til hva som var attraktivt for 20 år siden, ønsker vi imidlertid i dag det motsatte. Uansett hvor ironisk det måtte fortone seg, er det driftsmessig optimalt at brukerstyret ligner på og oppfører seg som intelligente terminaler i stedet for som selvstendige maskiner.

Like fullt er det selvstendige, fullt bestykkede PCer som anskaffes i milliontall over hele verden. Og at PCen i hardwaremessig forstand harmonerer svært så dårlig med behovene, er bare halve historien. Avstanden mellom egenskaper og behov er enda større på programvare-residen. Fenomenet lar seg bare delvis forklare via en kombinasjon av historie, motstand mot forandring, misforståelser og kostnader. Vi har analysert en rekke sider av saken ved tidligere anledninger,⁵ og lite har forandret seg utover at vi registrerer voksende interesse for ekte tynne klienter (Windows-terminaler) i markedet.

Hjelp i sikte

Situasjonen har fortsatt langs en negativ spiral – ikke bare driftsmes-sig, men i like stor grad sikkerhetsmessig. Kontroll er en forutsetning for forutsigbarhet, pålitelighet og sikkerhet, og PC-arkitekturen inviterer til det motsatte. Og der hvor det finnes et problem, dukker det gjerne opp løsninger som over tid utvikler seg til å avhjelpe, om ikke eliminere problemet. I dette tilfellet er løsningen programvareproduk-ter som effektivt overtar kontrollen over utstyret, reduserer brukernes

⁴ Tall fra Forrester Research, 1. kvartal 2004.

⁵ Se for eksempel "Windows-terminaler: Penger å spare?" i Mellvik-Rapporten nr. 109 og "Hvordan Microsoft og Sun drepte den tynne klienten" i nr. 108.

handlefrihet til et forhåndsbestemt nivå og holder løpende kontroll med både forandringer og aktiviteter.

Dagens produktgenerasjon er nr. 3 for flere av disse produktene, der noen har opprinnelse som verktøy for distribusjon og installasjon av programvare, mens andre har hatt kontroll og funksjons-låsing som hovedmål fra starten av. I dag karakteriseres verktøyene av database-drevne styrings-, kontroll-mekanismer, med voksende funksjonalitet: Programvare/lisens-kontroll, installasjon, sikkerhetskopiering, avviks-rapportering, oppdateringer og oppgraderinger – og så videre. I kombinasjon med katalogtjenester (typisk Active Directory) kan klientene styres individuelt eller i grupper, mens tradisjonelt tidkrevende oppgaver utføres over nettverket når brukerne ikke er til stede, og uten at driftspersonellet bidrar med annet enn overvåking.

Dette scenariet høres ut som en drøm for driftsmiljøer flest, og er mer en beskrivelse av hva som er mulig enn hva som er den faktiske situasjonen, selv for miljøer som har hatt denne type verktøy i drift i flere år. Poenget er at tilgjengeligheten av riktige verktøy er nødvendig, men ikke tilstrekkelig for å komme over i en situasjon som kan kalles 'under kontroll'. Utfordringene på veien dit er ikke først og fremst tekniske – i alle fall ikke med dagens generasjon av verktøy. Det viser seg at selv i 2004 mangler mange organisasjoner policy og retningslinjer som gjør det mulig å introdusere det brukerne i første omgang oppfatter som restriksjoner. Og etter at det formelle er i orden, skorter det gjerne på evne til å selge inn forandringene som positive: Når hovedsansen i budskapet er 'du får ikke lenger lov til å ...', krever det både teft og pedagogisk innsikt for å gjøre forandringen til noe positivt for den enkelte.

Hvor står vi, hvor går vi?

Noen vei utenom finnes imidlertid ikke, og om det ikke er enkelt, finnes det nok av eksempler på at det er mulig. På lengre sikt ser vi at system-arkitekturen, spesielt på klientsiden, vil få bedre behovstilpassning, men det vil ta minst 5 år før slike klienter hører til regelen i stedet for unntaket. I mellomtiden vil vi være avhengige av slike lockdown-verktøy for å etablere og opprettholde kontroll over en klientpark som fortsetter å vokse med høy hastighet.

I undersøkelsen vi nevnte på foregående side, kommer det frem at resten av markedet – over 60% – i beskjeden grad har tatt grunnleggende steg for å begrense brukernes mulighet til å gjøre forandringer på eget utstyr og konfigurasjon. Mens mange har tatt i bruk verktøy for inventarkontroll og automatisk programvare-distribusjon, er klient- og brukerproblemer omtrent like dominante for driftsavdeling og helpdesk som for 2 og 4 år siden. Situasjonen her hjemme er omtrent den samme – med enda lavere markedsdekning for 'lockdown'-produktene, men til gjengjeld mindre organisasjoner og dermed færre skaleringsproblemer.

I tillegg til de driftsmessige argumentene for å introdusere slike kontrollsystemer, er sikkerhet – som vi var inne på innledningsvis – til-

strekkelig motivasjon i seg selv. De viktigste poengene i den forbindelse er:

- ✓ Brukerinstallert programvare – hele spekteret fra smarte programmer for optimalisering av Windows til fildelingsprogrammer og spill – er notoriske kilder til infeksjon og videreformidling av virus. Organisasjonens policy for PC-bruk skal eksplisitt forby slik selvinstallasjon.
- ✓ Bærbare maskiner fordrer en egen policy, ikke bare for hva som kan gjøres på og med maskinen, men også hva slags oppkoblinger som er akseptable og hvilke data som kan lagres lokalt. Likeledes er det rimelig å begrense tilgangen, slik at kun brukeren selv kan bruke utstyret – ikke familie, venner eller kolleger, og teknisk personell kun etter anvisning fra IT-avdelingen.
- ✓ Oppdateringer: Spesielt for bærbare er det nødvendig å holde strikt oppsyn med versjoner på verktøy og programvare for å opprettholde grunnleggende god sikkerhet.

Dette er typiske oppgaver som dekkes av den nye verktøygruppen, men igjen er det verdt å understreke hvor vanskelig det er å komme i gang dersom det ikke finnes tilfredsstillende regler og rutiner for gjennomføring, og at disse faktisk følges. At de eksisterer, men ikke følges er verre enn at de ikke finnes i det hele tatt.

Snarveier

Utallige bøker, rapporter og artikler som anviser metoder for å forbedre situasjonen, er tilgjengelige på markedet. Vi observerer et forhold som er fullstendig analogt med hva vi har hatt på sikkerhetsfronten i årevis: At beskjeden innsats kan frembringe vesentlige forbedringer. Det faktum at mellom 50 og 70% av alle PC-brukere fortsatt har 'administrator-' eller 'power user-' tilgang til egen maskin taler for seg selv. Og akkurat her er det naturlig å begynne – med en kombinasjon av enkle regler og sunn fornuft. Imidlertid er verktøyene på markedet både for kraftige og for rimelige i forhold til jobben de gjør, til at det kan anbefales å gå løs på oppgaven 'manuelt' eller med individuelle verktøy for hver enkelt funksjon.

Produkter og leverandører

Microsoft er naturligvis en viktig og betydningsfull aktør også i dette segmentet. Selskapet kommer i den interessante situasjon at de først selger grunn-systemet og en rekke tilleggsverktøy, for deretter å tilby et produkt som reduserer følgeskadene av dem. Riktignok har ingen bedre forutsetninger enn nettopp Microsoft for å komme i inngrep med systemene på riktig nivå, men selskapets verktøy er likevel tilbakestående i forhold til de argeste konkurrentene på flere områder.

Blant de viktigste aktørene i dette segmentet finner vi følgende:

- ✓ Novells ZenWorks var tidlig ute i segmentet og har gjennomgått vesentlige utvidelser de siste to årene.

- ✓ IBMs Tivoli og CAs Unicenter er gamle travere innen drift og systemadministrasjon som har fått de nødvendige tillegg for å gi full kontroll med klient-parken. Karakteristisk for verktøyene er at de egner seg best for store miljøer.
- ✓ Wyse er best kjent for sine terminaler og tynne klienter, og forsøker å utvide sitt nedslagsfelt gjennom programvareproduktet Alcatraz – se omtale i Mellvik-Rapporten nr. 112.
- ✓ PowerFuse fra Real Enterprise Solutions (RET) i Holland har hatt betydelig suksess i Citrix/WTS-miljøer, men er også et sterkt alternativ på egen hånd.
- ✓ Britiske AppSense har en annen tilnærming til problemstillingene enn de fleste andre i segmentet, og retter søkelyset mot applikasjoner og ytelse, med kontroll- og styringsmekanismer som elementer i denne ligningen.

Et forbigående problem?

Selv motsigelsen i dette scenariet er – som bileksemplet innledningvis satte fingeren på – at markedet først anskaffer fete klienter for deretter å bruke betydelige ressurser på å redusere deres funksjonalitet til et akseptabelt nivå. Dette er åpenbart en situasjon som ikke kan vedvare, men om interessen for reelle tynne klienter er voksende, er den fortsatt forbausende beskjeden.

Ved siden av markedets mer eller mindre naturlige sendrektighet, er den viktigste årsaken til tilbakeholdenheten at vi ser konturene av en fullstendig omlegging av klientarkitekturen i kjølvannet av overgangen til Web-tjenester. Denne forandringen har ikke engang leverandørene helt taket på enda, med den følge at de gjør sitt beste for å bevare status quo. Her er det tryggest å sitte på gjerdet til vi ser hvilken vei det bærer.

De modigste og teknologisk mest oppegående er imidlertid i full gang med moderniseringen av arkitekturen, og deres argumenter er enkle: Riktignok vet vi ikke hvilken vei det bærer, men vi vet at ingen revolusjoner kommer over natten. Hvorfor ikke spare penger og andre ressurser mens vi venter? Å investere i en klient-arkitektur som alle vet har gått ut på dato, er meningsløst så lenge det finnes alternativer. Hvor lang levetid alternativene har, blir en endeløs og umulig diskusjon der det tyngste argumentet blir: “Mer enn en teknologi-generasjon”, det vil si mer enn 3 år. Dersom investeringene vi gjør i dag lever i 3 år, er vi klare for en ny generasjon. Å sitte på gjerdet blir med andre ord den mest kostbare løsningen. ■