

ws 7 beschikbaar voor grote klanten

# kennis in de eigen praktijk op

uit één distributiepunt konden we maximaal driehonderd werkplekken tegelijk uitrollen.”

Dat laatste bleek interessante feedback voor het verantwoordelijke team bij Microsoft. Een mogelijke oplossing is het bijplaatsen van distributiepunten (fysieke servers). Reeuwijk ziet nog een andere optie: Microsoft is bezig met de bètaversie van service pack 2 voor System Center Configuration Manager. Wellicht is het mogelijk daarin de limiet van driehonderd werkplekken nog aan te passen.

**Intern mag Getronics dan blij zijn met Windows 7, het overtuigen van klanten is nog een ander verhaal.** Veel bedrijven hielden de afgelopen jaren hardnekkig vast aan het aloude Windows XP. In de zakelijke markt is Windows Vista dan ook, zachtjes uitgedrukt, geen doorslaand succes. Reeuwijk kan zich dat wel voorstellen: “Geen enkel bedrijf wil met een systeem werken dat op de pc thuis niet lekker draait. Maar het grappige is dat

Windows Vista op bedrijfssystemen over het algemeen beter presteert, omdat daar betere kwaliteit hardware en software wordt gebruikt. De meeste bedrijven komen daar nooit aan toe; ze beginnen er niet aan uit vrees dat het niet goed zal werken. Met Windows 7 zijn de ervaringen van de pers en bètatesters thuis heel anders. Ze slaken letterlijk een zucht van verlichting ten opzichte van Vista. Daarom merken we dat de ‘pull’ vanuit bedrijven bij Windows 7 veel groter is. Bovendien bieden we klanten vanaf september gelegenheid om makkelijk met de nieuwe versie te experimenteren.”

Voor veel bedrijven begint de tijd ook te dringen, meent Reeuwijk. “Steeds meer klanten kunnen het zich gewoon niet meer veroorloven nog langer op Windows XP te blijven zitten. Onze ervaring is dat je zeker een halfjaar tot een jaar nodig hebt om je goed voor te bereiden op de migratie naar een nieuwe werkplek. Als je nu nog twee of drie jaar op XP zou blijven zitten, heb je niet genoeg tijd

meer voordat de support helemaal afloopt.”

Getronics adviseert zijn klanten die nog met Windows XP en oudere versies werken al sinds maart dit jaar om niet meer op Windows Vista over te gaan maar meteen voor Windows 7 te kiezen. Het is bijna een ongeschreven wet dat zakelijk gebruikers er goed aan doen het eerste service pack van een nieuw Microsoft-product af te wachten. Linden: “Zelf heb ik dat klanten ook altijd geadviseerd: wacht tot anderen er de ergste ellende uit hebben gehaald. Maar dat zou nu niet

meer mijn advies zijn, want het werkt gewoon. Het is echt niet nodig op het eerste service pack te wachten.”

Wat Windows Vista ook parten heeft gespeeld, meent Reeuwijk, is dat belangrijke toegevoegde waarde, zoals Network Access Protection, vaak ook beschikbaar kwam voor Windows XP. In Windows 7 daarentegen zit compleet nieuwe technologie die niet zal doorsijpelen naar Vista, laat staan Windows XP. Een voorbeeld is Branche Cache, een soort BitTorrent-technologie waardoor medewerkers op kantoren zonder snelle netwerk aansluiting bij elkaar bestanden kunnen ophalen. Of Direct Access, dat zonder VPN vanuit huis of een hotelkamer toegang geeft tot bedrijfsservers. “Die gaan echt toegevoegde waarde bieden”, meent Reeuwijk. Ook de gebruikersinterface van Windows 7 met een nieuwe taakbalk is een “enorme verbetering” die veel prettiger werkt en de productiviteit verhoogt, leert de ervaring van de Getronics-medewerkers.

**Wachten op eerste service pack is bij Windows 7 niet nodig**

**Microsoft heeft bij de ontwikkeling van Windows 7 intensiever dan voorheen samengewerkt met bedrijven als Getronics, constateert Linden.** Daardoor zijn veel fouten en problemen volgens hem bij voorbaat verholpen. Ook leveranciers hebben eerder dan met Vista aangehaakt bij het ontwikkelingsproces. Den Houter: “In het begin waren er nog wel wat probleempjes met hardware. Uiteindelijk hebben we nu totaal geen driverproblemen met onze laptops. Dat is echt een wereld van verschil met Vista indertijd.”

De ervaringen met Windows 7 bij Getronics zijn dus overwegend positief, maar de testers stuitten toch op problemen. Volgens Den Houter waren ze op de vingers van één hand te tellen. Het grootste probleem trof gebruikers van de interne financiële portal en hield verband met de aangescherpte beveiliging in Windows 7. Reeuwijk: “De instelling van een bepaalde authenticatietechnologie in Windows 7 bleek veranderd te zijn. Hij werkte standaard alleen nog met de nieuwste, veiligste vorm van encryptie. In de Java-webserver van deze portal is deze encryptiemethode nog niet beschikbaar. Daardoor kon je niet inloggen op die portal.” In samenspraak met Microsoft is het probleem opgelost.

Geert Kelfkens/g.kelfkens@sdu.nl



**President Obama heeft een nieuw legeronderdeel aangekondigd: het cybersecurity-commando.**

**In plaats van M1 Abrams tanks met neokeramisch gelaagde pantsers en JSF's met elektro-optische doelzoekers staat ons nu een cyberslagveld te wachten.** Voorbeeldje: neem het commando over van de energievoorziening en je legt een heel land lam zonder een JSF op te laten stijgen, laat staan te moeten bouwen. Obama's cybersoldaten moeten een antwoord gaan geven op deze bedreigingen.

**Cybertsaar** Een land dat vele tientallen miljarden per jaar uitgeeft aan defensie-IT kan wel een cybersecurity-coördinator gebruiken. Dit als antwoord op de toenemende cyberaanvallen van onbekende vijanden. Die oorlog is overigens al aan de gang: sommige grootbanken hebben duizenden virusaan-

vallen per dag te verduren. De aanleiding voor deze nieuwe functie is een advies uit het Clingendael van Washington. Daarnaast zag Obama zich ook al bedreigd toen tijdens zijn campagne voor de presidentskandidatuur e-mails met positiepapers en reisschema's in handen van hackers kwamen. Gezien de grote mate van technologische kennis die benodigd is om dit commando te kunnen leiden, zijn er maar weinig mogelijke kandidaten om Obama's cybertsaar te worden – een handboek soldaat is hier niet afdoende.

**Het (k)oude oorlogsvoeren** Tijdens de Koude Oorlog was het leven simpel. Als de Russen met hun duikboten te dicht bij de Amerikaanse kust kwamen, werden er bommenwerpers afgetankt en op de startbaan gezet – ready for take-off. Dit zagen de Russen dan weer via hun satellieten en de duikboten weken uit. Dit kat-en-muisspel tussen de grootmachten verliep zonder tussenkomst van officiële politieke communicatie.

**Het nieuwe oorlogsvoeren** Er zijn legio cyberaanvallen waar je je tegen moet wapenen. Zoals aanvallen waarbij grote hoeveelheden verzoeken naar een website het ding totaal onbereikbaar maken. Vervelend als je wilt chatten met het prinselijk paar, gevaarlijk als die computers vitale onderdelen van een land in de lucht houden. Een dergelijke aanval vond plaats in Estland. Die aanval uit 2007 was hoogstwaarschijnlijk het gevolg van het verplaatsen van een gedenkteken dat nog uit het Sovjet-tijdperk stamde. Bij deze politieke cyberaanval werd gepoogd websites van diverse Estse organisaties, waaronder het parlement, banken en kranten, plat te leggen. Waren het de Russen? Geen idee, want die aanvallen worden uitgevoerd via vele computers van argeloze internetgebruikers die hun beveiliging niet op orde hebben. Bij het nieuwe oorlogsvoeren is de vijand onbekend en ongrijpbaar, de nietsvermoedende burger is een pion geworden in de nieuwe strijd. Of de zeer geavanceerde infiltratie van begin 2005

in de kernsystemen van het Griekse telefoonverkeer. De halve regering werd afgeluisterd: de premier en zijn vrouw, de burgemeester van Athene, de ministers van Defensie, Justitie, en Buitenlandse Zaken, Europarlementariërs, mensenrechtenactivisten, hoge ambtenaren van defensie, openbare orde, koopvaardij, buitenlandse zaken, de marine, ambassadepersoneel, etc. Toch is er geen spoor van de daders. Cybercrime in optima forma.

**Papierfabriek met afstandsbediening** Een ander belangrijke cyberbedreiging zijn de industriële controlesystemen voor procesbesturing. Deze systemen zijn tegenwoordig met internet verbonden om te profiteren van online informatie. Dat heeft zakelijke voordelen, maar herbergt grote gevaren. Dat dit geen fantasie is, bewijst een voorbeeld uit 2001 waarbij het kinderspel bleek om een complete papierfabriek op afstand te besturen, en dus ook lam te leggen. Dit soort industriële systemen is helemaal niet gebouwd om internet kwaadaardigheid te weren.

**Je identiteit of je leven!** Opvallend is een aanval van mei 2009 op een elektronisch medicatiedossier van de staat Virginia. Een hacker eiste 10 miljoen dollar losgeld in ruil voor ruim 8 miljoen patiëntendossiers en 35 miljoen doktersrecepten. Die informatie is goud waard omdat je er gemakkelijk identiteitsfraude mee kunt plegen. Een plaag die de Verenigde Staten alleen al 50 miljard dollar per jaar kost. Deze zaak werd dan ook onmiddellijk door de FBI opgepakt. De website werd offline gehaald en de back-ups afgestoofd.

**Ga hier links af, of toch rechts?** Een gps-ontvanger is voor de gek te houden door een sterker signaal te versturen in de buurt van de ontvanger. Maar ja, wie doet nu zoiets, en waarom? Gps heeft naast plaatsbepaling ook een heel nauwkeurige tijdsbepaling, en die kun je dan ook veranderen. Financiële transacties op de beurs maken nogal eens gebruik van de gps-tijdstempels zodat je precies weet wanneer een aandeel verkocht was, of precies hoe laat de valuta verhandeld werd. Als je dat kunt beïnvloeden, wordt je heel snel heel rijk. Daarnaast gebruiken air-traffic controllers gps om vliegtuigbotsingen te voorkomen. Redenen te over dus voor president Obama om in actie te komen.

**De beste verdediging is de aanval** President Obama wil graag cyberkennis in huis halen om gericht aanvallen uit te kunnen voeren als dat nodig is. De vijandelijke computer- of energienetwerken van de vijand zijn de doelen voor infiltratie, overname, en uitschakeling. Op vijandelijke raketsystemen moet ingebroken kunnen worden, zodat raketten niet eens weggelaten. Scheelt weer onderschepenen. Voordat het zover is, moet eerst het handboek soldaat omgeschreven worden in een computer manual. **Rald Kulk en Chris Verhoef** (VU Amsterdam)