



Hajo Schulz

Updates onder controle

Windows-updates optimaal configureren

Een Windows-installatie wordt zonder updates al snel een open deur voor malware. Niet iedere patch werkt meteen foutloos, maar met de juiste instellingen is een goed compromis tussen veiligheid en betrouwbaarheid mogelijk.

Windows-updates onder controle

WSUS-server als updatefilter	52
Windows 7 sneller nieuw installeren	56
Snelle installatie van Windows 8.1	60

Complexe software zoals een besturingssysteem is nooit helemaal foutloos te krijgen, dus is regelmatig onderhoud nodig. Updates van Windows zorgen voor een compatibiliteit met nieuwe hardware, strijken uitschieters van de ontwikkelaars glad of breiden het systeem zelfs uit met nieuwe functies. De belangrijkste taak van een update – en de reden dat je daar zonder een goed geweten niet onderuit kunt – is echter het wegwerken van fouten die door anderen onrechtmatig gebruikt zouden kunnen worden om toegang te krijgen tot je systeem en de bestanden.

Microsoft doet daarbij grote moeite om de illusie van een perfecte wereld in stand te houden: met de standaardinstellingen installeert Windows zijn updates automatisch en op een tijdstip dat je als gebruiker daar zo min mogelijk van merkt. Desondanks is het toch handig even over het updaten na te denken en de instellingen naar eigen wensen aan te passen.

Het artikel vanaf pagina 52 gaat over de Windows Server Update Services (WSUS). Die zijn eigenlijk bedoeld om het leven van een systeembeheerder makkelijk te maken, wanneer ze honderden computers moeten updaten. Je kunt een WSUS-server echter ook in een werkgroepomgeving gebruiken en daar een goed instelbare updatereferentie voor Windows 10 mee construeren.

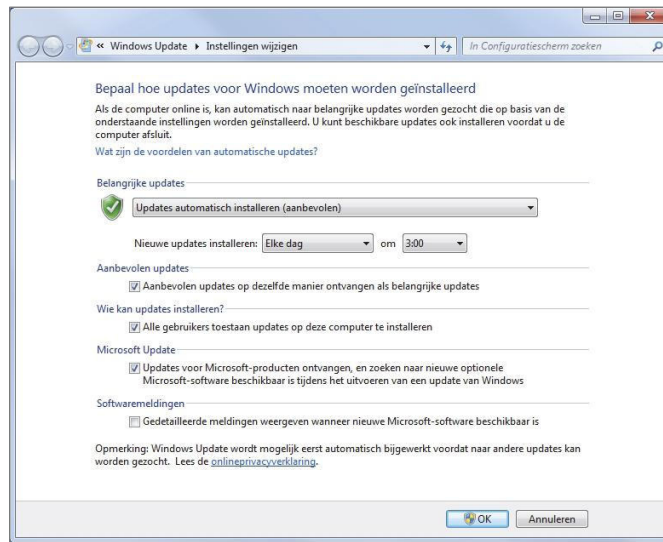
Als je tegenwoordig Windows 7 of 8 installeert vanaf een dvd die je jaren geleden gekocht hebt, is je computer vervolgens een eeuwigheid bezig om de updates te installeren die er in de loop der tijd bijgekomen zijn. De twee artikelen op pagina 56 en 60 laten zien hoe je dergelijke nieuwe installaties drastisch kunt inkorten en hoe je meteen bijgewerkte set-upmedia kunt maken om vaker te gebruiken.

Patch naar wens

Updates zijn hinderlijk, maar noodzakelijk. Daarom zijn de standaardinstellingen van Windows eigenlijk best zinnig: het systeem neemt de taak op zich om zichzelf regelmatig bij te werken, en doet dat zo geruisloos mogelijk op de achtergrond. Er zijn echter zeker ook redenen om wat meer controle over die activiteiten te willen houden – ook als die er niet voor niets zijn: als je het automatisch bijwerken uitschakelt, moet je regelmatig zelf aan de slag om het systeem bij de tijd te houden.

Een van de nadelen van een configuratie met volautomatische updates is dat die af en toe uitgevoerd worden als je ze helemaal niet kunt gebruiken: als tijdens een spannend ruimtegevecht de harde schijf opeens begint te reutelen of Windows uitgerekend tijdens een presentatie met belangrijke zakenpartners om toestemming vraagt om te herstarten, is dat lastig of zelfs pijnlijk.

Laat je alle updates automatisch installeren, dan krijg je ook alle fouten binnen die af en toe in de patches zelf zitten. Begin dit jaar had Microsoft blijkbaar grote proble-



Om de instellingen voor Windows Update bij Windows 7 of 8.1 te veranderen, heb je administratorrechten nodig.

men met de kwaliteitscontrole bij updates – in sommige gevallen werd een complete Windows-installatie onbruikbaar. Dergelijke ernstige fouten duiken gelukkig zelden op en worden dan snel aan Microsoft gemeld, zodat ze snel weer worden ingetrokken – op het moment dat hier in Europa de zon opkomt zijn ze vaak al weer verdwenen. Desondanks kan het zinvol zijn om het installeren van updates die niet meteen met veiligheid te maken hebben een paar dagen te laten wachten voordat je ze gaat installeren. Daarmee wordt de kans dat je een foute patch krijgt een stuk kleiner.

Een laatste argument tegen het volautomatisch updaten zijn de systeemherstarts die sommige patches nodig hebben. Als je je pc vaak 's nachts films laat hercoderen of grote bestanden laat downloaden, is het niet zo prettig als een herstart dat werk halverwege abrupt afbreekt. Ook een computer die in een thuisnetwerk als mediaserver dient, moet niet uitgerekend herstarten als de hele familie voor de tv zit om een film te kijken.

Als het er alleen om gaat om updates te verhinderen of een automatische update op onmogelijke tijden tegen te houden, helpt naast de hier genoemde configuratietrucs vaak ook een heel eenvoudige ingreep: laat Windows ruim op tijd voor de kritische actie handmatig naar updates zoeken. Dat geldt ook voor computers die maar af en toe aangezet worden en tussendoor wekenlang niet gebruikt worden.

Windows 7 en 8.1

De mogelijkheden om invloed uit te oefenen op het updaten verschillen aanzienlijk tussen de diverse Windows-versies. Windows 7 en Windows 8.1 delen de updatepakketten die door Microsoft beschikbaar gesteld worden in twee categorieën in: 'belangrijk' en 'optioneel'. In de eerste categorie hoort alles wat beveiligingslekken in het systeem dichtmaakt. Deze updates moet je zo snel

mogelijk nadat zo'n lek bekend wordt installeren. Bij de optionele updates zitten minder noodzakelijke updates zoals taalpakketten en het webframework Silverlight. Minder kritieke foutoplossingen en nieuwe drivers en compatibiliteitspatches worden door Microsoft op ondoordringelijke criteria ingedeeld als belangrijk of optioneel. Sommige krijgen het kenmerk 'aanbevolen'.

Op het tabblad 'Windows Update / Instellingen wijzigen' in het Configuratiescherm kun je instellen hoe deze belangrijke en aanbevolen updates geïnstalleerd moeten worden – niet aanbevolen optionele updates moet je altijd handmatig installeren als je ze nodig hebt.

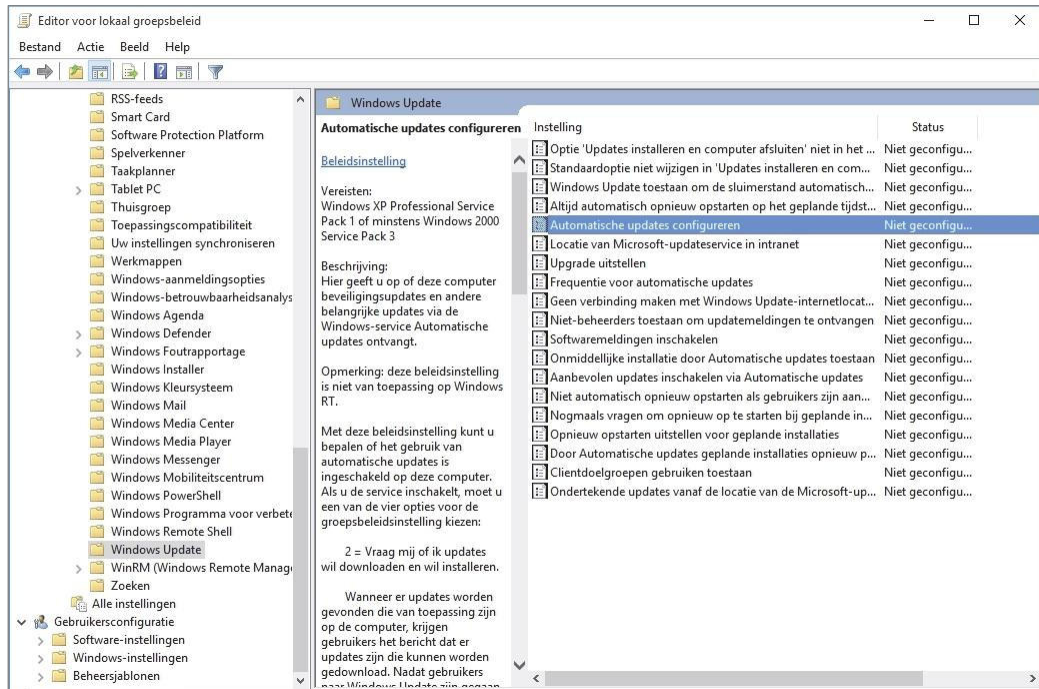
Normaal zoekt Windows eens per dag naar nieuwe updates en worden ze 's nachts om 3 uur geïnstalleerd. Als de computer op dat tijdstip uitgeschakeld is, wordt het installeren een minuut na het aanzetten ingehaald. Bij twee drop-downvelden op het instellingentabblad kun je de update-installatie beperken tot een bepaalde dag of op een bepaald tijdstip zetten.

Het grootste drop-downveld dient ervoor de volautomatische update-installatie uit te schakelen en in plaats daarvan een melding te krijgen als er een nieuwe update beschikbaar is, naar keuze voordat of nadat Windows die gedownload heeft. Het zoeken naar updates is hier ook helemaal uit te zetten, maar dat is niet aan te raden omdat je dan ook bij patches voor zware beveiligingslekken geen melding krijgt.

Windows behandelt aanbevolen updates op dezelfde manier als belangrijke. Als je de bijbehorende instelling uitvinkt, krijg je alleen nog een melding van nieuwe aanbevolen updates en moet je het installeren daarvan zelf in gang zetten.

Het vinden van de beste instelling voor jezelf is altijd een compromis tussen gemak, veiligheid en de wens zelf te bepalen wat het systeem wanneer doet. Wat de veiligheid van je gegevens betreft moet je het automatisch installeren van belangrijke

Het Groepsbeleid is eigenlijk voor administrators en bedrijfsomgevingen bedoeld. Een aantal daarvan is echter ook op computers van particulieren zinvol.



updates niet zonder meer uitzetten omdat daar niet alleen bugfixes bijhoren, maar ook het bijwerken van de virusdatabase van Windows Defender, die sinds Windows 8 als standaard virusscanner dient. Aanbevelen updates kun je met een gerust hart op 'handmatig' zetten en het installeren een paar dagen of tot de volgende patchday uitstellen om enigszins uit te sluiten dat die problemen op hun eigen systeem veroorzaken. Als je helemaal op safe wilt spelen, zoek je voor het installeren van dergelijke updates op internet naar het betreffende KB-nummer en kijk je of daar veel foutmeldingen over bestaan.

Detailinstellingen

Als het verplicht herstarten – dat na het installeren van een belangrijke update nodig kan zijn – een probleem is, kun je de werkwijze van Windows Update met behulp van het Groepsbeleid (Policies) bijstellen. Heb

je Windows Pro, Ultimate of Enterprise, dan kun je met de toetscombinatie Windows+R en het intypen van gpedit.msc de Editor voor lokaal groepsbeleid starten. De voor Windows Update relevante instellingen staan daar in het pad 'Computerconfiguratie / Beheersjablonen / Windows-onderdelen / Windows Update'.

Als je Windows 7 Home of Windows 8.1 Core hebt, moet je in plaats van het groepsbeleid met de Register-editor aan de slag, die je bijvoorbeeld start met Windows+R en regedit. Daar ga je eerst naar HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows en maak je een nieuwe sleutel aan met de naam WindowsUpdate als die nog niet bestaat. Daarin moet je een subsleutel maken met de naam AU.

De belangrijkste optie om via de Policies invloed op Windows Update uit te oefenen, heet bij de Editor voor lokaal groepsbeleid 'Automatische Updates configureren'. Dat groepsbeleid moet geactiveerd zijn om ervoor te zorgen dat Windows rekening houdt met de hieronder beschreven Policies. Voor het inschakelen is uit de lijst een van de mogelijke configuraties te kiezen: 2 staat voor 'Vraag mij of ik updates wil downloaden en vraag mij na het downloaden of ik de updates wil installeren', 3 voor 'Updates automatisch downloaden. Vraag mij na het downloaden of ik de updates wil installeren', 4 betekent 'Updates automatisch downloaden en installeren volgens de opgegeven planning' en 5 'Lokale administrators kunnen de configuratiemodus voor Automatische updates voor berichtgeving en installatie van updates zelf kiezen.' – dan geldt datgene wat je in het Configuratiescherm instelt.

Als je dat groepsbeleid via het Register wilt instellen, moet de gewenste instelling in een DWORD-waarde met de naam AUOptions in de boven genoemde sleutel AU staan. Als je voor optie 4 gaat, moet je bij de Editor voor het lokaal groepsbeleid nog een tijdschema daarvoor instellen: in het Register maak je daarvoor twee andere items in AU aan: de DWORD-waarde ScheduledInstallDay bepaalt welke dag de automatische updates uitgevoerd moeten worden, waarbij 0 voor iedere dag staat en 1 voor zondag, 2 voor maandag tot en met 7 voor zaterdag. De gewenste tijd is alleen in hele uren in te stellen: in de DWORD-waarde ScheduledInstallTime komt dan ook een getal tussen 0 en 23.

Om automatische herstarts door Windows-updates te verhinderen, zijn er twee verschillende manieren. De eerste is vooral handig als een pc lang bepaalde taken moet uitvoeren waarbij een gebruiker aangemeld blijft en af en toe een keer op het apparaat gaat kijken. Dan kun je de via een Policy of het Configuratiescherm ingestelde update op een bepaald tijdstip laten doorgaan, maar moet je het item 'Niet automatisch opnieuw opstarten als gebruikers zijn aangemeld na geplande installaties van Automatische updates' deactiveren. In het Register heet de bijbehorende DWORD-waarde NoAutoRebootWithLoggedOnUser die in de sleutel AU moet staan. Een 1 betekent dat dit actief is.

Als je automatische updates überhaupt verdacht vindt, schakel je over naar 'Vraag mij of ik updates wil downloaden en vraag mij na het downloaden of ik de updates wil installeren.' en activeer je het groepsbeleid 'Onmiddellijke installatie door Automatische updates toestaan'. Dat klinkt minder dramatisch dan het is: die regel zorgt ervoor



Na het updaten moet je vaak herstarten. Het is hinderlijk als dat automatisch gebeurt en de computer opstart terwijl hij nog dingen aan het doen is.

dat kleine updates die geen diensten onderbreken en geen systeemherstart nodig hebben in ieder geval automatisch geïnstalleerd worden. Bij die updatepakketten horen onder andere de virusupdates voor Windows Defender – dan heeft de virusscanner in ieder geval altijd de laatste virussignatures, ook als andere security-patches nog op hun installatie wachten. In het Register staat die instelling in een DWORD-waarde met de naam `AutoInstallMinorUpdates` en de inhoud 1 in de sleutel AU.

Voor alle wijzigingen aan het groepsbeleid – of dat nu via de officiële editor of rechtstreeks in het Register is – geldt dat die niet meteen werken, maar blijkbaar eerst bij Windows moeten doordringen. Wat daar precies voor zorgt was niet te reproduceren. Een aanroep van `gpupdate /force` hielp in ieder geval niet. In sommige gevallen leidde een herstart van Windows er zelfs niet toe dat de nieuwe instelling ook in het Configuratiescherm zichtbaar werd. Een paar uur later was dat wel het geval.

Windows 10

Bij Windows 10 zitten de instellingen voor Windows Update bij de 'Instellingen'-app op het tabblad 'Bijwerken en beveiliging / Windows Update / Geavanceerde opties'. De mogelijkheden om invloed uit te oefenen op de automatische updates beperken zich daarbij tot een paar dropdownvelden. Is daar 'Automatisch (aanbevolen)' geselecteerd, dan start Windows na het installeren van updates de computer opnieuw op als zijn gebruiker een tijdlang geen activiteiten ontplooid heeft. Het alternatief heet 'Melding om opnieuw opstarten te plannen'. Daarmee heb je tot twee dagen de tijd om het systeem zelf te herstarten voordat Windows dat doet.

Een onderscheid tussen belangrijke, aanbevolen en optionele updates is er niet meer. Dat zou hier ook niet zoveel nut hebben omdat Microsoft voor Windows 10 geen verschillende pakkettypen meer levert. Op de maandelijkse patchdays krijg je alleen nog een cumulatieve update die alle veranderingen bevat die tot dat moment toegevoegd zijn – zowel op het gebied van beveiliging als minder belangrijke. Daar horen ook nieuwe drivers en updates voor andere software van Microsoft bij, waaronder Office. Bijzonder kritieke security-patches die Microsoft zo belangrijk vindt dat ze niet tot de volgende patchday kunnen wachten, kunnen er altijd nog zijn. Het installeren daarvan weigeren of uitstellen is sowieso niet aan te raden.

De Editor voor lokaal groepsbeleid heeft bij Windows 10 nog alle instellingen die er ook bij oudere Windows-versies zijn. Bij onze experimenten werkte alleen het inschakelen van de meldingen voor of na het downloaden betrouwbaar, het automatisch updaten niet. Dat is echter niet aan te raden: de Defender kwam ondanks het groepsbeleid 'Onmiddellijke installatie door Automatische updates toestaan' soms geen virusupdates.



De instellingsopties van Windows Update zijn bij Windows 10 aanzienlijk beperkter. Bij een Home-versie kun je upgrades niet eens tegenhouden.

De optie om automatisch herstarten te verhinderen als een gebruiker aangemeld is gezien de mogelijkheid je via de instellingen twee dagen de tijd daarvoor te geven, is redelijk overbodig geworden. Het lijkt er al met al op alsof het Groepsbeleid voor Windows Update er alleen nog is om bij bedrijven de samenwerking met een WSUS-server te regelen. In dezelfde gedachtegang klopt het dat de boven beschreven Register-aanpassingen bij Windows 10 Home helemaal niets lijken te doen: volgens de officiële Microsoft-documentatie is die versie niet in staat om via WSUS bijgewerkt te worden.

Een update-instelling die er in Windows 10 bijgekomen is en waar je in ieder geval even over na moet denken, zit achter de link 'Kiezen op welke manier updates worden geleverd' op de instellingenpagina. Als je die aanklikt, krijg je de mogelijkheid in te stellen of Windows Update zijn pakketten alleen van de servers van Microsoft moet halen of ook van andere computers in het lokale netwerk of op internet. De keerzijde van de medaille: iedere pc die op die manier updates binnenhaalt, wordt automatisch een server voor dezelfde kring van machines. De instelling om updates via het lokale netwerk te verspreiden is overal zinvol waar meerdere computers een enkele internetverbinding delen en je daar dus niet telkens dezelfde bestanden mee binnen hoeft te halen. Bij dergelijke omgevingen kan de standaard ingestelde optie om updates ook over internet te verspreiden dan voor flink wat extra data-verkeer zorgen.

Upgrades

Bij het verschijnen van Windows 10 heeft Microsoft aangekondigd dat dit het laatste versienummer is. Toekomstige vernieuwingen zullen niet meer als nieuwe Windows-versies verschijnen, maar zullen in de vorm van gratis upgrades voor Windows 10 verspreid

worden zodra ze klaar zijn. Windows Update bekommert zich ook om het installeren van die upgrades.

In welke mate je invloed kunt uitoefenen op het installeren van die upgrades, hangt ervan af welke Windows-versie je hebt. Microsoft stelt dergelijke upgrades eerst ter beschikking aan de deelnemers van het Insider-programma (<https://insider.windows.com>). Als je die testversie van Windows gebruikt – niet geschikt voor productiesystemen – moet je ermee leven dat je upgrades kunt krijgen die nog niet helemaal foutvrij zijn. Je kunt alleen kiezen tussen een snelle en een langzame upgrade-ring. Bij de slow ring krijg je een update pas als bij de fast ring is gebleken dat hij goed is.

Als een upgrade in het Insider-programma lang genoeg getest is en door Microsoft rijp wordt bevonden, gaat hij naar de betalende Windows 10-klanten. Voor de Home-editie geldt: slikken of stikken. Upgrades worden daar geïnstalleerd zo gauw Microsoft ze uitbrengt, zonder dat je daar enige invloed op hebt. Bij Windows 10 Pro, Enterprise en Education kun je met de optie 'Upgrades uitstellen' het tijdstip van installatie nog vier maanden uitstellen. Op de lange termijn hou je de upgrades echter niet tegen – in ieder geval niet zonder Windows Update moedwillig buiten werking te stellen en daardoor ook geen security-updates meer te krijgen. Je kunt voor de verschillende upgrades geen aparte installatietijdstippen instellen.

Bij bedrijven met een infrastructuur met een eigen updateserver, kunnen administrators het installeren van upgrades nog eens acht maanden uitstellen om ze in de eigen omgeving eerst grondig te testen. Die 'Current Branch for Business' zit in alle Windows 10-versies met uitzondering van Home.

Voor omgevingen waarin gecertificeerde Windows-installaties jarenlang onveranderd moeten draaien, is er bovendien de 'Long Term Servicing Branch'. Windows-installaties krijgen dan geen functionele upgrades maar alleen security-updates. Microsoft definieert alle twee tot drie jaar een nieuwe actuele feature-stand. Klanten kunnen er dan voor kiezen of ze die gebruiken of bij de vorige versie willen blijven. Microsoft garandeert maximaal tien jaar support voor LTSB-versies, dan moeten die ook bijgewerkt worden.

Het uitstellen van upgrades verhindert het installeren van updates niet. Microsoft maakt eindelijk een consequent onderscheid tussen die twee begrippen: upgrades hebben nieuwe functies, updates lossen fouten op en dichten beveiligingslekken. Zakelijke klanten die updates desondanks eerst zelf grondig willen testen voordat die bij de gebruikers geïnstalleerd worden, kunnen ze met een WSUS-server klaarzetten. Daardoor hebben ze meer mogelijkheden voor het controleren en configureren ervan. Hoe je dat doet, en hoe je dat ook bij je thuisnetwerk of in een klein bedrijf kunt doen, staat in het volgende artikel. (nkr)

www.ct.nl/softlink/1512048

ct