

Standaard beschouwt Windows XP elke gebruiker als Beheerder. Dit geeft gebruikers én programma's die gebruikers starten, het recht om (andere) programma's te installeren en de systeemconfiguratie aan te passen. Spyware, virussen en wormen maken helaas dankbaar gebruik van deze verregerende vrijheid. U voorkomt veel beveiligingsproblemen door de computer te gebruiken zonder maximale rechten. In deze workshop leest u hoe u dit aanpakt.

Dat Windows XP de mogelijkheid biedt gebruikeraccounts aan te maken en elke gebruiker een eigen werkomgeving te geven, is bekend. Dat elke account ook kan worden gekoppeld aan een gebruikersprofiel dat voor die gebruiker bepaalt wat wel en wat niet mag, is minder bekend. Gevolg: bijna iedereen die Windows XP gebruikt, is Beheerder of Administrator. Voor de beveiliging van de computer is dit rampzalig. Elke gebruiker kan onbeperkt foute keuzes maken en dat geldt ook voor opgestarte programma's. Een programma erft namelijk de rechten van de persoon die het opstart. Wie dus als beheerder een webpagina opent met een Trojan-horse in de code of een email opent met

Minder rechten,

Veiliger werken zonder beheerdersrechten



een virus, geeft malafide code de mogelijkheid het register of systeembestanden en mappen aan te passen. Met alle schadelijke gevolgen van dien. De oplossing voor dit probleem is de verschillende gebruikers te voorzien van verschillende rechten. En belangrijker: voor het dagelijkse gebruik van de computer, zoals het schrijven van een email of het surfen over internet, nóóit gebruik te maken van een account met rechten van de computerbeheerder. De account van de Administrator mag eigenlijk alleen worden gebruikt in absolute noodgevallen. Het is een goede gewoonte om voor het reguliere computerbeheer een nieuwe account te maken en er alle rechten aan te geven. Dit account kunt u dan enigszins aanpassen aan de eigen wensen, terwijl de Ad-

ministrator-account volledig standaard blijft. Raken ooit de rechten van de nieuwe beheerders-account kwijt, dan kunt u deze bovendien via de Administrator-account herstellen. Een andere eenvoudige, maar praktische maatregel is om de bureaubladachtergrond van de beheeraccount te veranderen in een egale, opvallende kleur. Dat herinnert u er later steeds opnieuw aan dat u met de beheeraccount werkt en zo snel mogelijk na het afronden van de beheerklusjes moet uitloggen, om risico's te verkleinen.

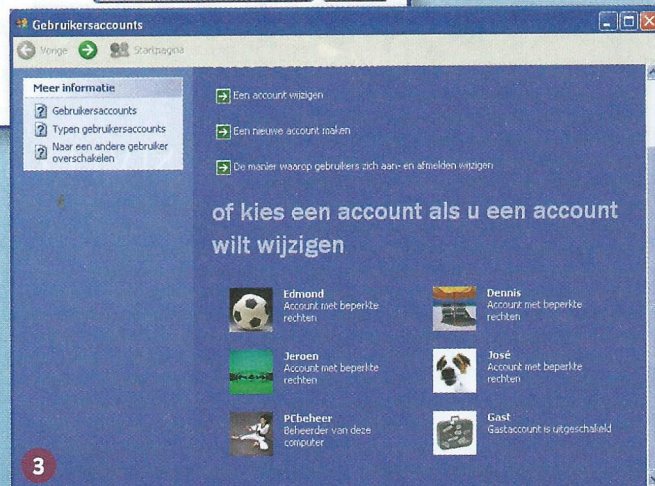
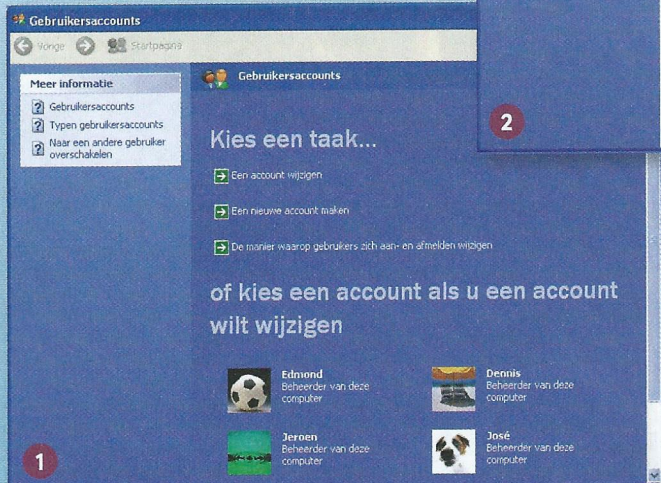
PROBLEMEN BIJ MINDER RECHTEN

Niet meer computeren als Administrator is eenvoudig en met een paar klikken te realiseren.

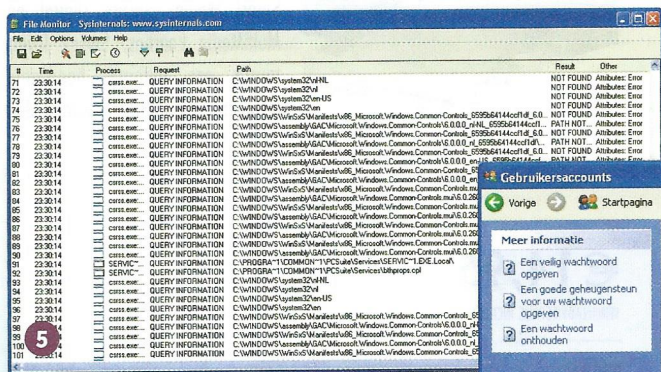
Geheel probleemloos zal het gebruik van de computer hierna niet meer zijn. Bepaalde programma's starten niet meer, bijvoorbeeld omdat ze toegang eisen tot afgeschermd delen van het register. Ook het installeren van een programma of het gelijk zetten van de klok is niet meer vanzelfsprekend. In dit artikel leest u hoe u

Gebruikers onder andere Windows-versies

Ook onder Windows 95, 98 en Me is het mogelijk meerdere gebruikersaccounts aan te maken en elke gebruiker een eigen werkomgeving te bieden. Wat echter ontbreekt is de mogelijkheid met rechten te werken: elke gebruiker beschikt over alle rechten. Het werken met verschillende gebruikersprofielen waaraan rechten gekoppeld zijn, is voorbehouden aan de 'NT-versies' van Windows: NT, 2000 en XP.



minden nico!



Windows XP voor dagelijkse taken kunt gebruiken zonder rechten van de computerbeheerder. Ook laat het zien hoe u veelvoorkomende problemen, veroorzaakt door een beperkte account, oplost. Een veiliger computer is het resultaat.

AAN DE SLAG

Genoeg theorie. De kans is groot dat u en uw medegebruikers – al dan niet ongemerkt – gebruik maken van Administrator-accounts. Alle accounts die tijdens de installatie van Windows worden aangemaakt, hebben deze maximale rechten (afbeelding 1), maar ook alle accounts die u later via het Configuratiescherm toevoegt. Om veilig te werken is het verstandig om een extra account aan te maken, dat u gebruikt voor het beheren van de computer. Verder moeten alle accounts waarmee gebruikers inloggen om de computer gewoon te gebruiken, worden omgezet naar minder rechten. Open het Configuratiescherm en kies het onderdeel Gebruikersaccounts. Kies eerst voor het maken van een nieuwe account. Geef dit de naam van het nieuwe beheerderaccount, bijvoorbeeld 'PCBeheer' en bevestig dat het account behoort tot het type Computerbeheerder. U bent nu terug

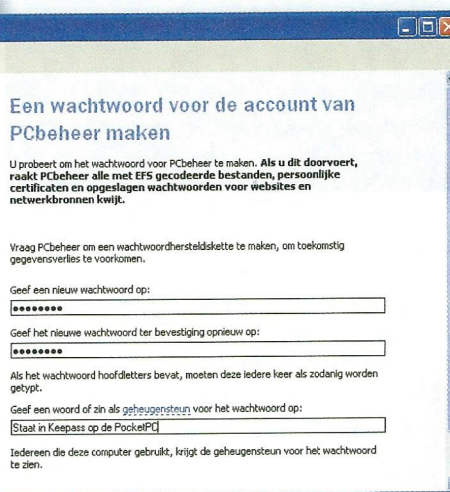
in het onderdeel Gebruikersaccounts. Hier staan alle accounts opgesomd die al op de computer zijn aangemaakt. De meeste daarvan zullen het bijschrift Beheerder Van Deze Computer hebben. Open elk account en kies voor Het Type Account Wijzigen. Selecteer de optie Beperkte Mogelijkheden en klik op de knop Het Type Van Een Account Wijzigen (afbeelding 2). Herhaal dit voor alle accounts, behalve voor de account PCBeheer (afbeelding 3).

WACHTWOORDEN INSTELLEN

Minstens zo belangrijk als het instellen van de juiste rechten, is het instellen van een wachtwoord, minimaal voor de accounts met beheerderrechten. Klik daartoe op elk account en

VOORBEREIDING

Voordat u de gebruikersrechten aanpast is het verstandig de programma's waarvan u weet dat ze gebruikt gaan worden, op voorhand te installeren. Installeer daarna nog alle updates voor Windows en individuele programma's. Maak vervolgens eventueel een schijfimage van de volledige installatie, met Norton Ghost of Easy Computing True Image.



kies Een Wachtwoord Instellen. Geef een nieuw wachtwoord op en bevestig het in het tweede vak (afbeelding 4). Als geheugensteun kunt u een woord of zin opgeven. Het is niet noodzakelijk om voor de gebruikersaccounts met beperkte rechten wachtwoorden in te stellen. Dit is afhankelijk van of u met meerdere gebruikersaccounts werkt of alleen één account deelt, en of u documenten en bestanden van

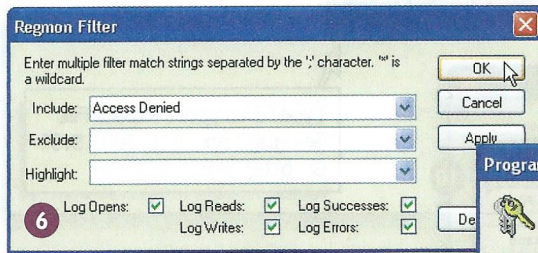
de verschillende gebruikers voor elkaar wilt afschermen.

PROBLEEMSOFTWARE

Helaas laat sommige software zich niet installeren met een beperkt gebruikersaccount, zodat u gedwongen bent om alsnog gebruik te maken van een Administrator-account. Vaak wordt dit veroorzaakt doordat het programma zich niet houdt aan twee essentiële regels om als niet-Administrator te kunnen installeren. Allereerst mogen er tijdens de installatie geen bestanden worden geplaatst in de map Program Files van de Windows-systeemmap (doorgaans C:\Program Files) en in de Windows-map (doorgaans C:\Windows). Daarnaast mag het programma geen registersleutels aanpassen in de sleutel HKEY_LOCAL_MACHINE. Deze kennis helpt gevorderde gebruikers om zulke software alsnog te kunnen installeren. Met het gratis programma FileMon kunt u controleren welke mappen worden aangesproken door het programma (afbeelding 5). In eerste instantie houdt FileMon alle wijzigingen bij. Het is dan ook aan te raden om tijdens het installeren van een probleempakket – waarbij u FileMon gebruikt om te achterhalen welke mappen worden aangesproken – zo min mogelijk andere toepassingen te openen. Daarnaast gebruikt u de zoekfunctie (Edit / Find) om activiteiten van het betreffende

WACHTWOORD VOOR DE BEHEERDER

Windows XP vraagt u tijdens de installatie een wachtwoord op te geven voor het account van de Administrator. Met die account logt u in door in het Welkomstscherm met de verschillende accounts tweemaal Ctrl+Alt+Del in te drukken. De gebruikersnaam om in te loggen is het Engelse Administrator, ook in de Nederlandse versie. Gebruik het wachtwoord dat u tijdens de installatie hebt opgegeven. Onder XP Home Edition is het Administrator-wachtwoord standaard blanco; een druk op Enter volstaat om ermee in te loggen. Inloggen als Administrator is onder XP Home Edition alleen mogelijk in de Veilige Modus. Om in te loggen start u de computer opnieuw op en drukt u tijdens de start van Windows op F8.



installatieprogramma op te sporen. Een vergelijkbaar programma, RegMon, kunt u vervolgens gebruiken om te controleren welke registersleutels worden benaderd. Standaard registreert RegMon alle bewerkingen van het register. Het is aan te raden om na installatie van het programma te kiezen voor File / Capture Events, zodat logging wordt uitgeschakeld en u rustig via Edit / Find op zoek kunt naar de sleutels waarin wijzigingen zijn aangebracht door de betreffende installatiesoftware. Bovendien kunt u de resultaten filteren. Kies voor Options / Filter of druk op Ctrl+L. In het vak Include typt u Access Denied (afbeelding 6). Hierdoor wordt het logresultaat uitgedund. Met deze informatie kunt u vervolgens de rechten van zowel de mappen als van de registersleutels aanpassen, zodat deze ook door een niet-Administrator mogen worden aangepast. Verderop in dit artikel, bij 'Probleemoplossing via het register', leest u hoe u de rechten van sleutels aanpast. Hoewel u pas in de praktijk merkt welke software extra aandacht nodig heeft, vindt u online een overzicht van programma's waarvan bekend is dat u ze niet als niet-Administrator kunt installeren.

Vooral games leveren vaak problemen op bij het uitvoeren als niet-Administrator. De kopieerbeveiliging is hiervan vaak de oorzaak. Weigert een spel te starten, met de melding dat u de originele spel-cd in de cd-romspeler moet leggen, terwijl u dat al hebt gedaan? Microsoft heeft onlangs SafeDisc uitgebracht, een gratis fix die dit probleem verhelpt. De fix SafeDisc van Microsoft werkt echter niet bij alle games. Voor een grote hoeveelheid games bestaan eigen NoCD-patches, die het spel of het programma aanpassen zodat er niet meer om de cd wordt gevraagd. Door een dergelijke patch toe te passen, kunt u ook vaak omzeilen dat de software niet kan worden gestart.

UITVOEREN ALS

Een oplossing voor programma's die niet willen starten wanneer de gebruiker niet over de rechten van de Administrator beschikt, is met de rechtermuisknop op het programma te klikken en in het menu te kiezen voor Uitvoeren Als. In



het volgende venster kiest u de account die wel over voldoende rechten beschikt. Na het opgeven van het wachtwoord is een druk op Enter voldoende om het programma toch te starten (afbeelding 7).

Voor programma's die u vaak gebruikt en die deze rechten nodig hebben, is het raadzaam een maatoplossing te maken. Dit kan door het commando RunAs te gebruiken, de equivalent van Uitvoeren Als. RunAs wordt gestart vanaf de DOS-prompt of via Start / Uitvoeren, en vraagt dan het wachtwoord dat bij de account hoort waaronder het commando moet worden gestart. Vervolgens maakt het een nieuw proces aan met de rechten van de opgegeven account. Een voordeel van RunAs is dat u het eenvoudig in snelkoppelingen kunt gebruiken. Programma's die altijd andere rechten nodig hebben kunnen zo eenvoudig altijd met die rechten worden gestart. Start u bijvoorbeeld als gebruiker zonder Administrator-rechten via Start / Uitvoeren met het commando CMD een DOS-prompt, dan hebt u ook binnen die prompt maar beperkte rechten. Start u de prompt echter met runas /user:PCbeheer cmd, dan hebt u na het

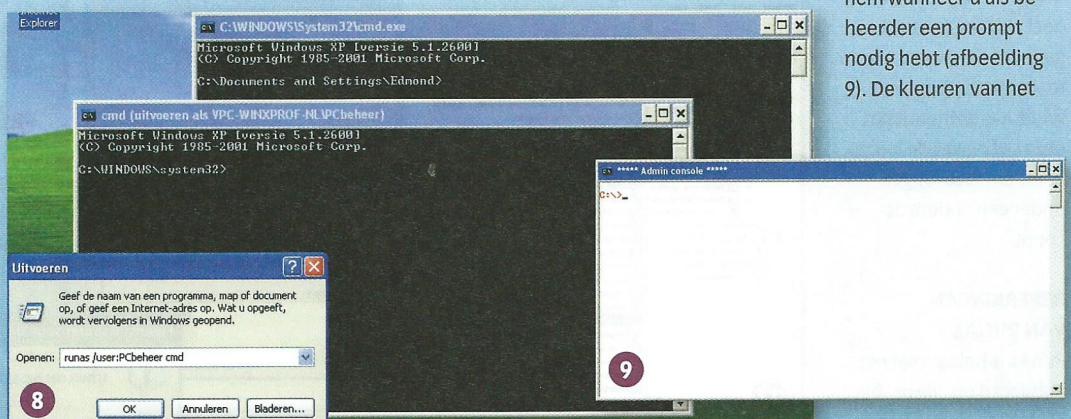
WISSELEN ZONDER WELKOM

Voor Snelle gebruikerswisseling is het inschakelen van het Welkomstscherm van Windows XP noodzakelijk. Maakt u liever gebruik van het klassieke aanmeldvenster, maar wilt u toch gebruik maken van Snelle gebruikerswisseling? Via een registertruc lukt het. Zorg vooraf voor een goede backup van het register en belangrijke bestanden. Schakel eerst het Welkomstscherm (en daarmee Snelle gebruikerwisseling) uit via het onderdeel Gebruikersaccounts in het Configuratiescherm. Kies Start / Uitvoeren en typ Regedit. Blader naar de sleutel HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Klik met rechts op AllowMultipleTSSessions en kies Wijzigen. Geef een 1 op in het vak Waardegegevens. Verlaat het register via Bestand / Afsluiten. Druk vervolgens op Ctrl+Shift+Esc om Taakbeheer op te roepen. Op het tabblad Gebruikers klikt u met rechts op de gebruikerssessie die u wilt verlaten en kiest u Verbinding Verbreken. Vervolgens meldt u zich via het klassieke aanmeldvenster aan met de andere gebruiker. Schakel terug via Taakbeheer en de optie Verbinding Maken (te bereiken door met rechts op de gebruiker te klikken).

opgeven van het juiste wachtwoord een prompt mét beheerrechten (afbeelding 8). Het is overigens raadzaam om bij gebruik van de prompt als beheerder, deze een ander uiterlijk te geven, dat u erop attendeert dat het een prompt is met maximale rechten. Maak daarom een snelkoppeling met de volgende opdracht:

```
C:\Windows\system32\runas.exe /u:PCbeheer
"%windir%\System32\cmd.exe /k cd c:\ && color fc
&& title ***** Admin console *****"
```

Voeg deze speciale snelkoppeling toe aan het menu Start en gebruik hem wanneer u als beheerder een prompt nodig hebt (afbeelding 9). De kleuren van het



BLIK IN DE TOEKOMST

Met de komst van Windows Vista, de opvolger van XP, wordt voortaan anders omgegaan met gebruikeraccounts. Standaard zal de gebruiker over aanzienlijk minder rechten beschikken. Zelfs als u gebruikmaakt van een Administrator-account, blijven uw rechten beperkt. Deze aanpak wordt mogelijk doordat de meeste onderdelen van het besturingssysteem prima kunnen worden bediend met een account met beperkte rechten, in tegenstelling tot bij Windows XP. De noodzaak om een Administrator-account te gebruiken valt grotendeels weg. Daarnaast zijn sommige instellingenvensters voorzien van een knop waarmee u de huidige account tijdelijk 'opwaardeert' met Administrator-rechten, om zo de wijziging alsnog door te voeren.

venster zijn rood op wit, in plaats van het gebruikelijke wit op zwart.

Gebruik van het commando RunAs is afhankelijk van het actief zijn van de Secondary Logon Service. Werkt RunAs niet zoals verwacht, controleer dan of deze service wel is gestart, via een rechtsklik op Deze Computer / Beheren / Services en Toepassingen / Services. Deze onderdelen laten zich overigens alleen wijzigen via een account met beheerrechten. Tenzij u de individuele delen opstart via het RunAs-commando. Met `runas /user:PCbeheer "mmc c:\windows\system32\compmgmt.msc"` start u bijvoorbeeld Computerbeheer met de rechten van het PCbeheer-account. Zo kunt u de computer toch beheren via een tijdelijke 'opwaardering' van uw rechten.

Gebruikers van Windows XP Professional genieten bij het gebruik van het commando RunAs het voordeel van de extra schakeloptie /savecred (save credentials). Door deze toe te voegen aan een commando hoeft alleen de eerste keer dat het betreffende onderdeel via RunAs wordt uitgevoerd een wachtwoord te worden opgegeven. Windows onthoudt dat deze gebruiker de macht heeft om in te loggen onder een andere account.

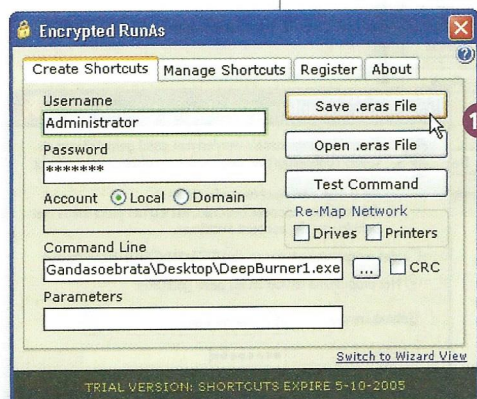
BEPERKINGEN VAN RUNAS

RunAs is helaas niet het antwoord op alle problemen. Windows Verken-

ner, dat u beter niet als Administrator gebruikt tenzij het noodzakelijk is, laat zich via RunAs niet aansturen. De oorzaak is dat Explorer.exe, ofwel Windows Verkenner, tijdens de start controleert of er al een versie van zichzelf actief is. Aangezien de Windows Shell ook Explorer is, voegt deze zich direct naar de rechten van de geopende sessie. Het is dus niet mogelijk om bijvoorbeeld een map te delen via RunAs, tenzij een omweg wordt bewandeld. Start Internet Explorer met beheerrechten via `runas /user:PCbeheer "C:\Program Files\Internet Explorer\iexplore.exe"`. Zodra het is gestart, typt u als adres C:\ in de adresbalk en drukt u op Enter. Blader nu naar de map die u wilt delen en klik erop met de rechtermuisknop. Doordat het proces nu verloopt via de met beheerrechten geladen Internet Explorer, is het mogelijk de map te delen. Via ditzelfde venster kunt u ook naar C:\Windows\System32 navigeren en daar als beheerder alle individuele onderdelen van het Configuratiescherm starten.

VERSLEUTELDE ADMINISTRATOR-GEGEVENS

De schakeloptie /savecred kent als groot nadeel dat de aanmeldingsgegevens in niet-versleutelde vorm worden opgeslagen. Het is daardoor eenvoudig om te achterhalen welke gebruikersge-



Type: Encrypted RunAs File
Gewijzigd op: 3-10-2005 8:36
Grootte: 346 bytes

vens bij de Administrator-account horen. Voor wie de computer met anderen deelt kan dit een bezwaar zijn. Met het programma eRunAs hebt u dit probleem niet, doordat het de aanmeldingsgegevens versleuteld opslaat (afbeelding 10). U maakt een versleuteld RunAs-bestand en geeft hierbij de gebruikersnaam en het wachtwoord op van de Administrator-account. Er wordt vervolgens een eras-snelkoppeling aangemaakt, waarmee u de toepassing als Administrator kunt starten. U kunt een gratis proefversie downloaden. De werking van de snelkoppelingen in deze versie is beperkt tot drie dagen. Eenmaal geïnstalleerd, geeft u op het tabblad Create Shortcuts bij de invoervakken Username en Password de aanmeldingsgegevens van de Administrator-account op. Bij Command Line klikt u op de knop Bladeren en wijst u het programma aan dat u wilt opstarten met aangepaste rechten. Plaats vinkjes bij Drives en Printers in het groepsvak Re-Map Network, als u via de andere account ook toegang wilt tot schijven en printers die normaal gesproken bij een specifieke account horen. Klik tot slot op Test Command om de instellingen te testen en op Save .eras File om de snelkoppeling aan te maken.

UW COMPUTER BIJWERKEN

Windows Update verplicht u gebruik te maken van een Administrator-account om de computer bij te werken. De opdracht RunAs biedt geen soelaas. Wilt u per se Windows Update bezoeken, dan kunt u gebruikmaken van Snelle gebruikerswisseling, om tijdelijk over te schakelen naar Administrator-rechten. De beste oplossing is gelukkig eenvoudiger: zorg ervoor dat Automatische updates is ingeschakeld. Hiermee blijft het systeem up-to-date doordat de updates op de achtergrond worden gedownload en geïnstalleerd. Ook bij niet-Administrators.

PROBLEEM OPLOSSEN MET GPEDIT

Een nogal vervelende beperking voor de gebruiker met beperkte rechten is dat deze niet is gemachtigd om de computertijd aan te passen (afbeel-

