PC-Gebruikersaccounts-Beveiliging

Waarom een **standaard**-account i.p.v. een **administrator**-account?

Presentatie door:

RvdH

Steenwijk, 18 oktober 2016
Zwolle, 20 oktober 2016

Doel

Het systeem beter bestand maken tegen onheil van buitenaf en afschermen tegen onbedoelde wijzigingen.

Voor wie?

Voor de Windowsgebruiker(Vista, 7, 8 of 10) met een pc, laptop of tablet.

Nieuwe computer.
Als internet, mailen, bankieren, skypen, etc. werkt, zijn we blij.

De virusscanner, firewall en wifi met wachtwoord, alles in orde.

Ons kan niets gebeuren en we wanen ons veilig.

Toch hebben we niet alles voor elkaar.

De meeste gebruikers werken met een zgn **administrator**-account ipv een **standaard**-account.

Dit gaat min of meer automatisch.

Wat is dan het verschil?
Alles gaat toch goed??

Een vergelijking met de auto.

Hoe doen we het met de auto?

We rijden rond, tanken en kleine klusjes aan de auto doen we zelf.
Voor onderhoud gaat de auto naar de garage.

De automonteur ontgrendelt de motorkap, die zit normaal op slot.
Hij doet het onderhoud, olie verversen, oud oliefilter eruit, nieuw oliefilter erin, etc.
Als de monteur klaar is doet hij de motorkap weer dicht en de auto op slot.
Niemand kan er dan nog bij.

De automonteur doet bij z'n eigen auto de motorkap ook dicht en de auto op slot.

Niemand kan bij de auto, er is altijd toestemming nodig.

Hoe doen we dat met de computer?

Het onderhoud doen we meestal zelf, dat gaat prima.

Maar we rijden **zonder** motorkap.

Iedereen kan bij de motor.

Ze kunnen bv. zand in de motor gooien of
een klemmetje (ransomware) met een code op de benzineleiding zetten.
Tegen betaling kun je dan de code krijgen (mag je hopen).
Bedenk maar wat allemaal mogelijk is.

Bij de auto is dit niet normaal, maar bij de computer doen we dat wel!!
De openstaande "motorkap" is niet zichtbaar en Windows waarschuwt niet.

Het is als rijden zonder autogordels of de voordeur niet op het nachtslot doen.
Normaal gaat het altijd goed, maar zo af toe hoor je wel eens dat iemand een aanrijding heeft of een inbreker op bezoek heeft gehad.

Nu zegt u:
Ik heb toch een virusscanner en firewall die beveiligen toch alles?
Dat klopt.
Maar zie de virusscanner als een bodyguard die voor de auto staat en iedereen moet tegenhouden.
Helaas moet hij wel eens naar het toilet of moet op bijspijkercursus(update).

En een wachtwoord dan?
Die werkt alleen bij het opstarten van de pc.

Wat wil de computercrimineel?

Vroeger was hij bezig met verstoren of schaden in de vorm van reparatie en tijdverlies.

Tegenwoordig wil hij geld verdienen.

Dat doen ze onder andere door:

Bestanden te blokkeren (ransomware) en dan losgeld te vragen.
Misschien krijg je na betaling van het losgeld een unlockcode om de de blokkering op te heffen.
Momenteel is het een sterk groeiende business.
Er zijn "firma's" die voor een paar honderd euro een ransomwarepakket leveren.
Zie c't Magazine mei 2016, blz 80.

Geld overboeken met behulp van jouw bankgegevens, DigiD of creditcardnummers.
Op slinkse manier verkregen door te vragen of mee te kijken in de pc met een keylogger.

Kortom de pc moet goed beveiligd zijn.

Waardoor kunnen we een besmetting oplopen?

- Op een link klikken in een verdachte mail. Die mail kan afkomstig zijn van een voor jou bekend adres.

- Soms zijn van vertrouwde sites de advertenties besmet, in april 2016 was dat het geval. Klikken op een besmette link.

- Over een link schuiven met de muis kan soms al een besmetting geven.
  Dit doen we vaak om te zien wat het adres is van de site.

- We zijn iets te nieuwsgierig of te snel en klikken toch op een link.

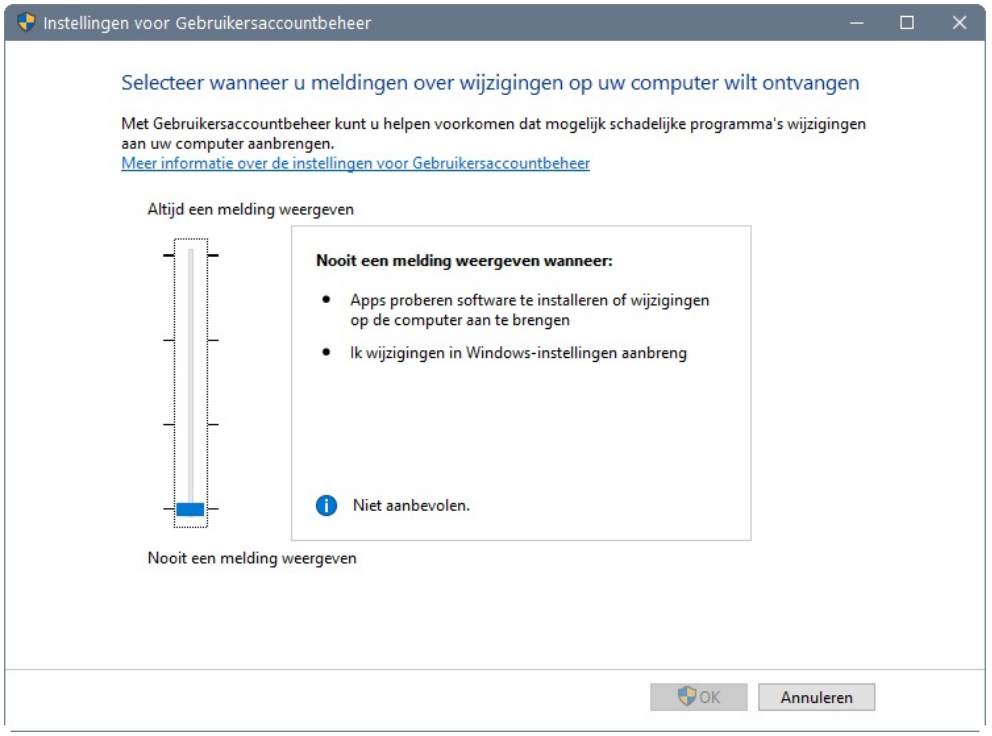
- Programma's, spellen of sites hebben een dubbele agenda.
  Een leuke bovenkant, maar onder water klopt het niet.

Allemaal bekende zaken mag ik aannemen.

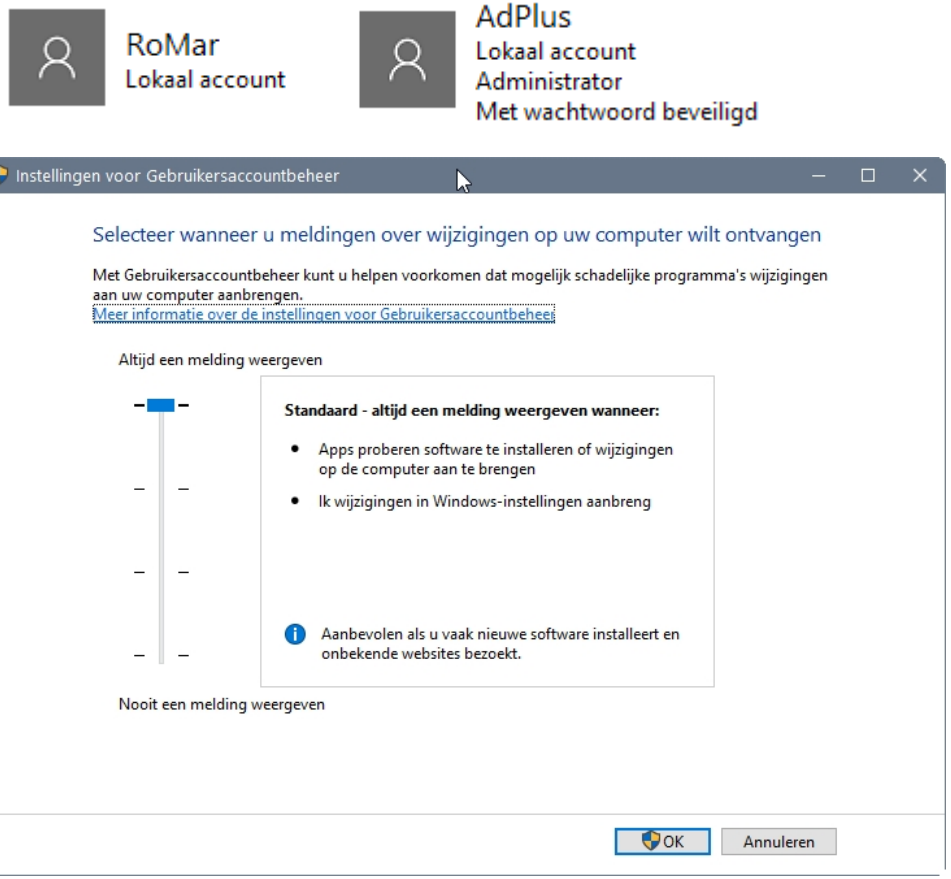
Jarenlang heb ik het zo gedaan.

RoMar
Lokaal account
Administrator

Voordeel geen gezeur over "mag ik dit installeren" etc.
Nadeel toch niet zo veilig, gelukkig geen last van gehad.



Ca 3 jaar geleden is het account RoMar gewijzigd in een standaard-account en is er een apart administrator-account AdPlus naast gemaakt.
Ruim een half jaar geleden ook aangepast bij een kennis.
Het bevalt tot nu toe allemaal goed.



Voordeel van een **standaard**- en een **administrator**-account naast elkaar op de pc:

- Betere bescherming van de pc.

- Andere gebruikers van de pc, zoals huisgenoten, familie, (klein)kinderen en/of bezoekers, kunnen niet liggen rommelen in de pc.

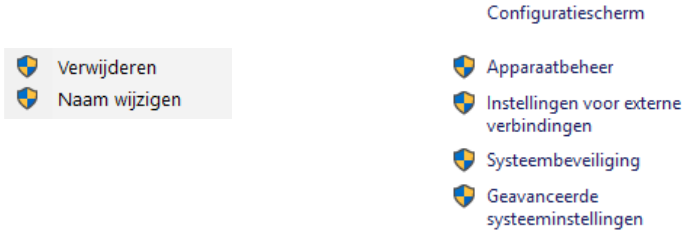
- Het is mogelijk om voor de standaardgebruiker zgn read-only of afgeschermde mappen te maken.
  De administrator heeft de normale mogelijkheden, terwijl de standaardgebruiker alleen kan lezen in deze mappen.
  Het is bv. niet mogelijk om files te verwijderen of te wijzigen.
  De map zit als het ware op slot.

  Hopelijk biedt dit ook bescherming tegen ransomware.
  Ik heb dat echter niet geprobeerd…..

Nadeel:

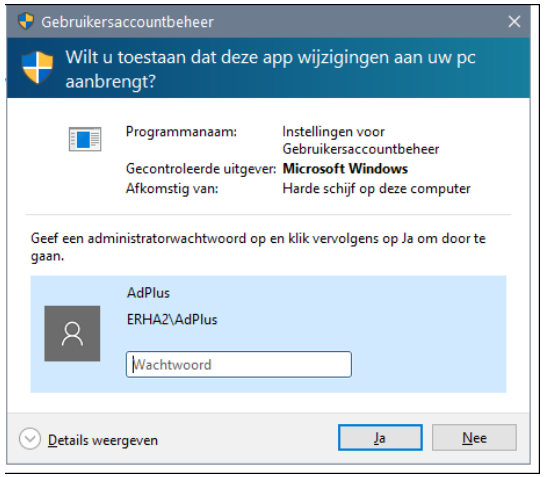
- Men moet zo af en toe een wachtwoord invullen.
  Even lezen, nadenken en dan, indien alles klopt, het wachtwoord van 4 of 5 letters/cijfers invullen en Enter.

Ingelogd als standaardgebruiker worden alle keuzes waar de onderstaande schildjes voor staan afgeschermd en moet het administratorwachtwoord ingetypt worden. Inloggen als administrator is niet nodig.

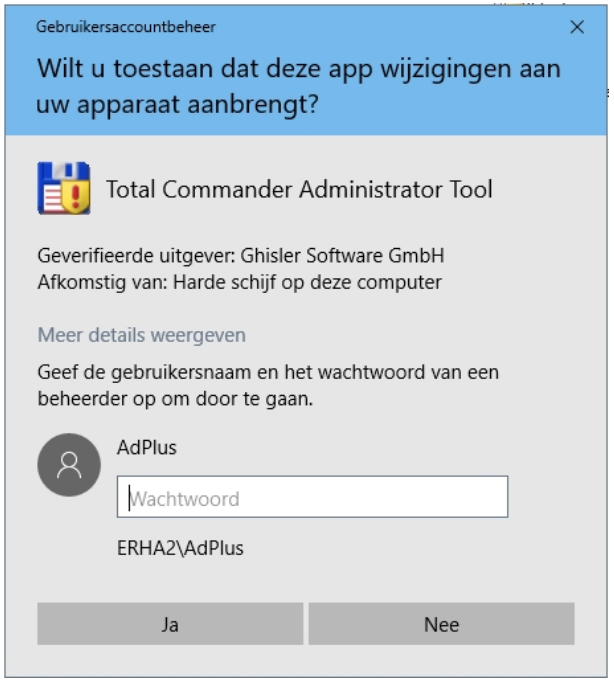


Onderstaand scherm verschijnt dan:

Windows 7, 8 en 10 (oud)



Windows 10 (nieuw)



Eigenschappen standaard- en administrator-account

Ingelogd met:	Standaard-account	Administrator-account
Normale programma's, mail, internet, skype, verkenner, office programma's, sommige virusscanners,	OK	OK
Eenvoudige en persoonlijke instellingen in Windows	OK	OK
Uitgebreide en algemene instellingen in Windows	Administrator-wachtwoord intypen noodzakelijk	OK
Programma's installeren of de-installeren, tools als AdwCleaner, CCleaner, HitmanPro, sommige virusscanners,	Administrator-wachtwoord intypen noodzakelijk, zie ook toelichting volgende blad	OK
Read-only of afgeschermde map	Lezen/kijken mogelijk, administrator-wachtwoord intypen noodzakelijk om iets te wijzigen	OK

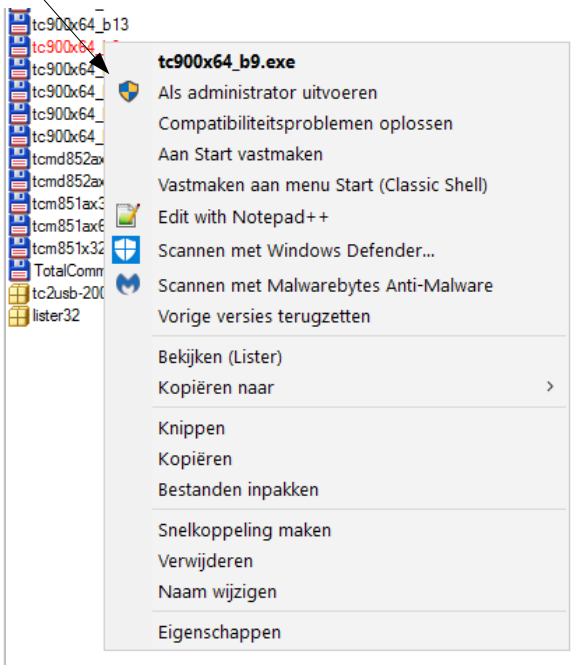
Installeermogelijkheden als je bent ingelogd als standaardgebruiker:

1 – Het setupprogramma vraagt zelf om het administratorwachtwoord.

2 – Het setupprogramma starten met administratorrechten,
met rechtermuisknop menu openen en dan op de regel met het schildje te klikken.

3 – Afmelden en inloggen als administrator, oa Canon wil dat bij
sommige installatieprogramma's. Daarna weer inloggen als standaardgebruiker.

4 – Tijdelijk het accounttype van de standaardgebruiker verhogen naar administrator en
deze na het installeren weer terug zetten.



Omzetten **administrator**-account naar een **standaard**-account in het kort:

1 – Een herstelpunt maken, is niet noodzakelijk.

2 – Schuif van Gebruikersaccountbeheer (UAC)
voor Windows 8 en 10 op bovenste positie en
voor Windows 7 op bovenste of tweede positie.

3 – Een lokaal administrator-account maken, met een eenvoudig wachtwoord.

4 – Alle normale gebruikers van administrator wijzigen in standaardgebruiker.

5 – Data Execution Prevention (DEP) aanvinken.

Zie verder , zie PC-GebruikersAccount-Instellen.pdf

Naast de standaard virusscanner (Windows Defender) scan ik regelmatig met:

HitmanPro (handmatig dagelijks) en **HitmanPro.Alert** (real time)
HitmanPro scant de computer razendsnel (nog geen 5 minuten),
HitmanPro.Alert vertraagt het opstarten van programma's enigszins.
Het is niet gratis.
site:
http://www.surfright.nl/nl/home

AdwCleaner
is een (gratis) programma waarmee u op eenvoudige wijze allerlei ongewenste toolbars, browserextensies, browser hijackers kunt verwijderen van uw computer.
Bij de 1e scan komen er veel meldingen te voorschijn, even opletten wat u verwijdert.
site:
https://toolslib.net/downloads/viewdownload/1-adwcleaner

Malwarebytes Anti-Malware
is een (gratis) anti-spyware-programma.
De effectiviteit van het programma wordt door velen geroemd.
site:
https://nl.malwarebytes.com

Enkele opmerkingen:

- Een besmette pc komt altijd ongelegen.
  Net als het plat gaan van de harde schijf of Windows, altijd vlak voordat we de backup zouden gaan maken.

- Na gijzeling helpt alleen een recente backup.
  Hopelijk heb je de geblokkeerde bestanden niet in de backup gezet.

- Mijn persoonlijke tip:
  Bewaar uw DigiD en bank inloggegevens en wachtwoorden niet in de pc of in de cloud, maar gewoon op een stukje papier ergens in huis.
  Digitale kluisjes zijn misschien moeilijk te kraken, maar bevatten lekken of worden slecht beheerd.
  Hoe vaak liggen gegevens van personen niet op straat, bv bij Yahoo, Isala.

- De ransomware-"industrie" wordt steeds groter.
  Voor een paar honderd euro zijn ransomware-pakketjes te koop.

- Ten op zichtte van jaren geleden zijn we nu altijd online en kunnen we niet zo goed zien wat de pc doet.

- Huidige computercriminaliteit is te vergelijken met het maatschappelijk probleem fietsdiefstal.

Tot slot:

- De normale gebruikers merken niets van deze wijzigingen, alleen degene met de monteurspet op wel, die moet wel eens een wachtwoord intypen.

- Nieuwsgierigheid is moeilijk te beveiligen, een extra drempel, in de vorm van een wachtwoord, kan dan helpen.

- Het mag duidelijk zijn dat deze wijzigingen geen garantie zijn tegen onheil. Windows bevat nog genoeg lekken en gaten, maar een hele grote is nu dicht.

- Bij mij kan niets gebeuren denkt u misschien, dat overkomt alleen mijn buurman. Helaas denkt die hetzelfde en de buurman aan de andere kant denkt dat ook. Een gewaarschuwd mens telt voor twee.

Bronnen:

– Artikel "Werk veilig" in SoftwareBus, nr 2014-6, blz 10.
Softwarebus is een uitgave van CompUsers, een HCC interessegroep.

– c't Magazine mei 2016, blz 80-91.

– SchoonePC
https://www.schoonepc.nl/windows10/werken_met_gebruikersaccounts.html

– Stukje tekst betreffende accounttype Windows: