Windows: Het systeem

D. Leeuw

21 juli 2025
0.0.0

1 Windows ontdekken

Of je nu programmeur, helpdesk medewerker, systeembeheerder, hacker of security officer bent het is handig om te weten hoe een systeem werkt. Als programmeur is het essentieel om te weten welke functies een systeem je aanbiedt zodat je er gebruik van kan maken. Als hacker is het goed om te weten wat het systeem je biedt en wat de vaak voorkomende fouten zijn die programmeurs maken. Voor helpdesk medewerkers is het handig als je meer weet van de werking van een systeem zodat je makkelijker de fouten van gebruikers snapt en voor systeembeheerders is de kennis van de interne werking van een operating systeem nodig zodat het systeem en de bijbehorende software op een juiste en veilige manier geïnstalleerd kan worden. Ten slotte is het voor de security officer essentieel om al deze voorkomende zaken te begrijpen, zodat een juiste security analyse gemaakt kan worden.

We beschrijven in dit stuk de globale werking van het Windows besturingssysteem.

Besturingssytemen en software in zijn algemeen, wordt vaak beschreven in lagen, in het Engels layers. Een stapel van deze layers wordt in het Engels dan een stack.

De meest simpele vorm van een besturingssysteem stack is:

1. user applications
2. operating system
3. hardware

hardware zijn de fysieke, tastbare, onderdelen van een computer. Hierbij horen CPU, geheugen, opslagsystemen, etc.

operating system ook bekent als OS, is een verzameling software die de hardware aanstuurt in opdracht van programma's (applications).

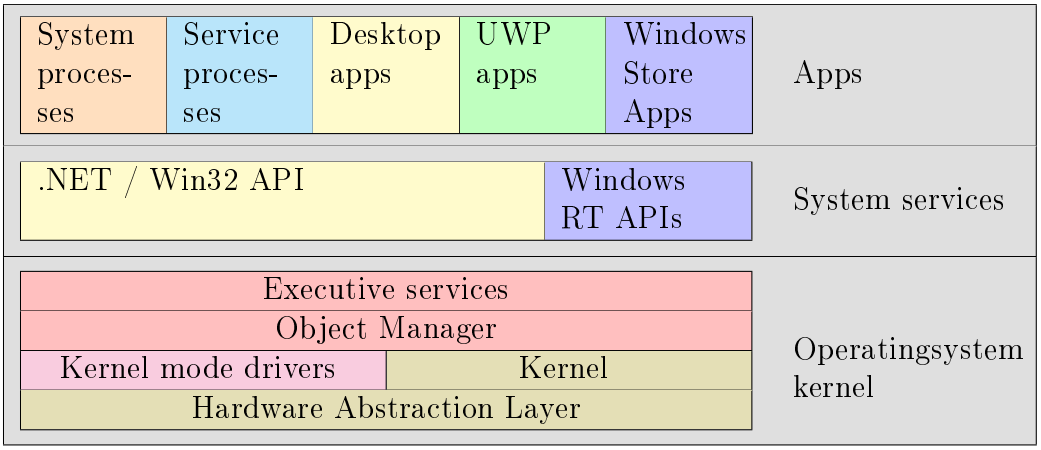
user applications ook bekent als apps, zijn de stukken software die wij, de gebruikers, gebruiken, zoals Microsoft Office.

De reden van het opdelen in lagen heeft meerdere redenen. Allereerst maakt het een complex geheel dat een operating system is overzichtelijk en makkelijker te begrijpen. Een andere reden is om te laten zien wat er afhankelijk is van elkaar. Bij operating systems heeft het ook te maken met een stukje veiligheid. Het operating system kan en mag tegen de hardware praten, terwijl user applications dat nu juist niet mogen. Het operating system bepaalt wie er wanneer toegang heeft tot een bepaald stuk hardware,

waar data in het geheugen zit en waar applicates. Als elke applicatie dat afzonderlijk zou kunnen bepalen zou het een zooitje worden. Het is de taak van het besturingssysteem om te zorgen dat alle taken op een computer op een nette manier worden afgehandeld.

1.1 Windows Architectuur

Om een idee te krijgen hoe een Windows systeem in elkaar steekt is er hieronder een in een stack globaal weergeven hoe een Windows systeem eruit ziet.



1.2 API

Een API is een afkorting van Application Programming Interface. Zoals de naam al aangeeft maakt een API het voor een ontwikkelaar mogelijk om tegen de API te praten en gebruik te maken van de functies die door deze API aangeboden worden. Een ontwikkelaar hoeft daardoor niet alle details te weten van het onderliggende systeem, maar zich enkel te richten op de functies van API. Voor de systeem ontwikkelaars is het handig want die hoeven zich niet bezich te houden met de programma ontwikkelaars, zolang als ze de API maar intact laten mogen ze daar onder alles wijzigen zonder dat er applicaties stuk gaan.

Een API is dus niets anders dan een beschrijving van hoe een stuk software aangesproken wil worden, een API kan dan ook van een library, framework of process zijn.

2 Applications

2.1 Services

Services is de Microsoft benaming voor processen. Processen draaien op de achtergrond en hebben geen grafische interface. Er is ook geen user interaction nodig om deze processen te laten draaien.

system processes essentiele processen voor het normaal functioneren van het operating system. Het afsluiten (al dan niet met opzet) van één van deze processen zorgt bijna altijd voor een system crash (voorbeelden: `lsass.exe`, `winlogon.exe`, `services.exe`).

service processes processen die niet essentieel zijn voor de werking van het OS. Draaien bijna altijd via `svchost.exe`.

2.2 Apps

Computers met Windows client operating systems worden gebruikt door gebruikers en deze gebruikers maken gebruik van applicaties (applications) zoals bijvoorbeeld Microsoft Office om hun werk te kunnen doen. Deze applicaties zijn niet standaard onderdeel van het besturingssysteem. Ze worden los van het OS geïnstalleerd. Applicaties hebben een grafische interface.

Desktop apps Traditioneel gebruiken desktop applications, zoals MS Office, de Win32 APIs en .NET.

Windows Store apps De Microsoft Store is een online plek waar je software, al dan niet gratis, kan downloaden. Windows Store apps, zijn dan ook die applicaties die je via de Microsoft Store kunt vinden en downloaden. De applicaties maken gebruik van de Windows RT API.

UWP apps Sinds Windows 10 is er de UWP (Universal Windows Platform, wat een door ontwikkeling is van de Windows RT APIs. Applicaties die ontwikkeld zijn om gebruik te maken van de UWP kunnen gebruik maken van zowel .NET, de Win32 API en de Windows RT API.

3 System services

De Windows System Services levert de APIs waar applicaties tegen praten. Ze communiceren nooit direct met de hardware. Het direct met de hardware praten is voorbehouden aan de kernel.

Windows kent verschillende APIs die door applicaties gebruikt kunnen worden.

Win32 De tradionele set DLLs (Dynamic Loadable Libraries) gebruikt door Windows applicaties zoals Microsoft Office.

.NET Een open source framework voor Windows, Linux en Mac OS X om voornamelijk web-based applicaties te ontwikkelen zoals Office365. Vooral bekent van de C# programming language.

Windows RT API Windows Real Time Application Programming Interface (WinRT) is een technologie die applicaties ondersteund die cloud-, touchscreen- en web-enabled zijn. De API is voor het eerst geïntroduceerd in Windows 8.

WSL WSL is het Windows Subsystem for Linux.

4 Kernel en drivers

De kernel van Microsoft Windows is de de NT OS Kernel (`ntoskrnl.exe`). De kernel is de basis van een besturingssysteem en het deel dat geladen wordt door de bootloader. De kernel is uiteindelijk verantwoordelijk voor het volledig en op een correcte manier opstarten van het hele systeem. De kernel bevat de basis hardware drivers en kan eventueel extra kernel mode hardware drivers laden. De kernel kunnen we opsplitsen in een aantal lagen of onderdelen:

Executive is een collectie kernel-mode functies waarin een kernel voorziet. Het bestaat uit: I/O manager, IPC Manager, Virtual Memory Manager, Process Manager, PnP Manager, Power Manager, Security Reference Monitor en de Object Manager.

I/O manager Regelt alle Input en Output

IPC manager Regelt de communicatie tussen de processen (Inter Proces Communication)

Virtual Memory manager Regelt welke proces of applicatie welk stukje geheugen heeft en/of mag gebruiken

Process manager Regels alle processen op het systeem

PnP manager Regelt de Plug-n-Play devices

Power manager Regelt het power management systeem

Security Reference Monitor

Object manager uiteindelijk moeten alle modules door de object manager naar de kernel of een device driver.

kernel en drivers de interface tussen de hardware en de executive services.

Hardware Abstraction Layer Een abstractie laag die van een een complex samenraapsel van hardware een paar uniforme interfaces maakt. Zo hoeven de lagen boven de HAL niets te weten van allerlei verschillende soorten printers, maar is er één uniforme printer interface.

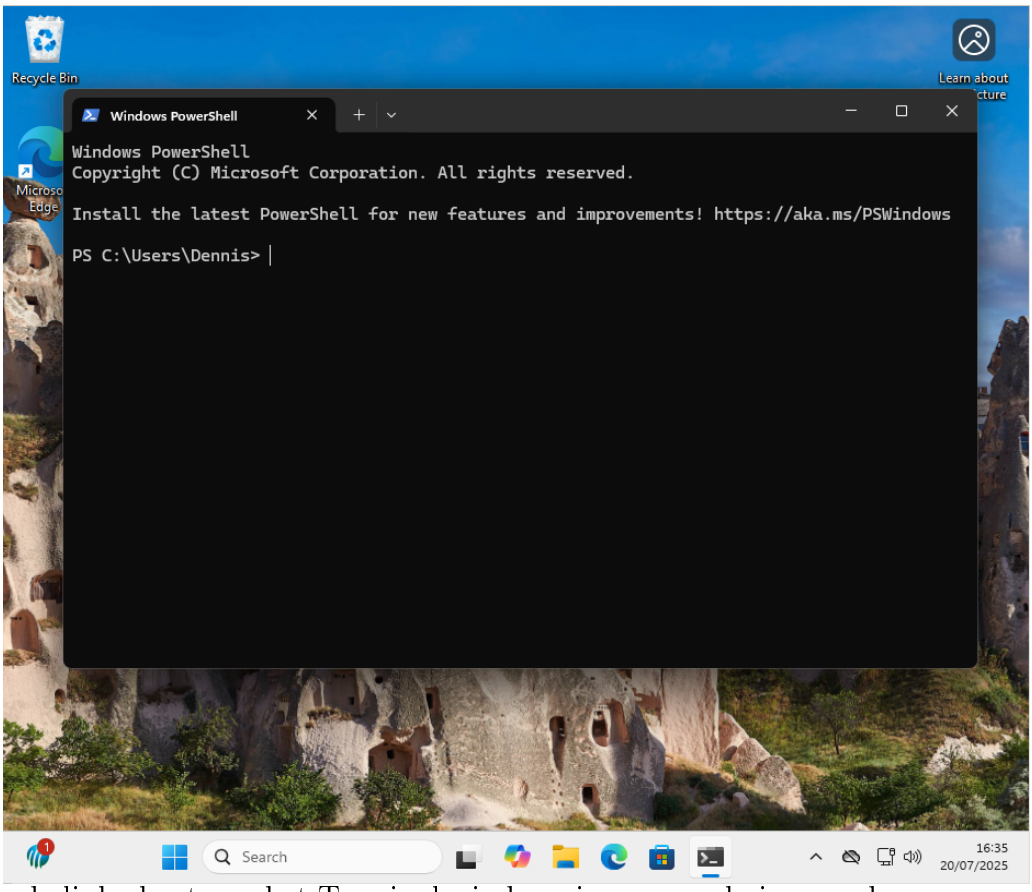
5 Command Line Interface

Naast de grafische interface is er op Windows ook een niet grafische interface die we meestal de Command Line Interface of CLI noemen. Met deze interface besturen we de computer niet met iconen, menus en de muis, maar via commando's die we via het toetsenbord intypen.

Voor windows zijn er twee omgevingen om gebruik te maken van commando's de eerste is de `cmd` of command omgeving, de andere is PowerShell. Je kan de command omgeving opstarten door in de zoekbalk `cmd` in te typen. Op dezelfde manier kan je `PowerShell` opstarten. Een laatste mogelijkheid is het opstarten van de `Terminal` applicatie die in Windows 11 automatisch zorgt dat je in PowerShell terecht komt.

5.1 De prompt

Als we terminal opstarten dan komen we in PowerShell terecht.



Aan de linkerkant van het Terminal window zien we een knipperende cursor. Voor deze cursor vinden we een regel die begint met PS, om aan te geven dat we in PowerShell werken. Als er niets staat dan maken we gebruik van `cmd`. Na de PS zien we C:, dit is onze C-drive. Je kunt je nu afvragen waar de A en de B-drive gebleven zijn. Dat is geen vreemde vraag. Het Windows besturingssysteem bestaat al lang en in een grijs verleden waren er floppy disks en deze disks moest je plaatsen in een, meestal ingebouwde, floppy drive. De eerste twee drive letters waren gereserveerd voor deze floppy drives. De eerste harddisk in een systeem kreeg daardoor de letter C en dat is altijd zo gebleven. De C-drive is de disk waarvan het systeem is opgestart. Hierop staat Windows op en alles wat daarbij hoort.

Het laatste stuk bestaat uit `\Users\Username`. Dit is het pad waarin je staat. Username is bij jou vervangen door de naam waarmee je ingelogd bent. Als je ingelogd bent als Administrator dan is het pad: `\WINDOWS\system32`. In de laatste geval adviseren zou je eigenlijk moeten uitloggen en inloggen als gewone gebruiker. Als Administrator heb je te veel rechten en kan je te veel stuk maken.

5.2 Werken met files en folders

De data op een disk (harddisk of SSD) is verdeeld over mappen, folders of directories. Deze namen worden door elkaar gebruikt, maar betekenen allemaal hetzelfde. Het zijn plekken waar bestanden of in het Engels files in kunnen worden opgeslagen zodat de data op de disk overzichtelijk kan worden ingedeeld. De directory waarin je nu staat is je home-directory, de plek waar jij je bestanden in mag opslaan.

Om de organisatie van data te bevorderen heeft Microsoft al een aantal subdirectories voor je aangemaakt. Type op de prompt `dir` en geef enter. Je krijgt nu een overzicht van bestanden en directories in jouw home-directory, zoals `Downloads`, `Documents`, `Music`, `Pictures`, `Videos` en nog wat meer. De hoop is dat gebruikers op deze manier hun data gestructureerd opslaan. Je hoeft je niet aan de structuur van Microsoft te houden. Als jij liever je data indeelt op basis van `Prive`, `School`, `Werk` kan dat natuurlijk ook. Alleen moet je dan nog wel zelf die directories maken.

Met het `mkdir` commando kan je een directory aanmaken:

```
mkdir Prive
```

Met het `rmdir` commando kan je een directory weggooien:

```
rmdir Prive
```

Directories die we met `rmdir` weggooien komen niet in de Recycle Bin terecht zoals dat wel gebeurt als je dat via `File Explorer` zou doen.

Je kan een directory alleen weggooien als deze leeg is. Alle default door Microsoft aangemaakte directories zijn niet leeg. Ze bevatten subdirectories of verborgen bestanden. Met de `-hidden` optie kan je met `dir` deze verbonden bestanden zichtbaar maken. Doen we een

```
dir Videos
```

Dan lijkt deze map leeg. Doen we echter:

```
dir -hidden Videos
```

Dan zie je dat er een bestand zichtbaar is geworden, namelijk een `desktop.ini` file.

We hebben gezien dat we met `rmdir` directories weg kunnen gooien. Met het `del` commando kan je bestanden weggooien, ook deze komen niet in de Recycle Bin terecht en zijn direct van het systeem verdwenen.

Om met mappen en bestanden om te kunnen gaan in PowerShell is er nog een commando nodig dat je veel zult gebruiken en dat commando is `cd`, wat een afkorting is van Change Directory. Daarmee kan je dus van directory wijzigen.

```
cd Documents
dir
```

De bovenstaande commando's zorgen ervoor dat je eerst jezelf verplaatst naar de Documents directory (LET OP: je prompt wijzigt mee) en met `dir` laat je zien welke files en folders er in deze directory staan. Je mag aan `cd` ook een volledig pad meegeven. Bijvoorbeeld

```
cd \Users
```

en met .. gaan we stapje dichter naar de basis van de harddisk, namelijk de root directory (\).

6 Directory structure

De manier waarop bestanden en mappen zijn ingedeeld op een disk noemen we een directory-tree. De tree begint bij de root. De root directory`root directory` is de directory die direct na de C: komt en wordt weergegeven door een enkele \. We kunnen snel daar de root-directory gaan met:

```
cd \
```

We staan nu aan het begin van de directory boom van de C-schijf. Met `dir` kunnen we zien welke directories er de eerste takken van de boom vormen:

```
PS C:\Users> cd \
PS C:\> dir


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----          7/8/2025   2:27 PM                inetpub
d-----          4/1/2024   9:26 AM                PerfLogs
d-r---          3/9/2025   3:10 PM                Program Files
d-r---          3/9/2025   3:00 PM                Program Files (x86)
d-r---          3/5/2025   5:05 PM                Users
d-----         7/20/2025   4:57 PM                Windows
```

6.1 \Windows

De `Windows` directory bevat alles wat bij het besturingssysteem behoort. Wijzigingen aanbrengen in deze tak van de directory tree kan je Windows

systeem mogelijk stuk maken. Maar het is wel goed om te weten wat je zoal in deze tak kan aantreffen.

Windows gebruikt extensies om aan te geven om wat voor soort bestanden het gaat. De extentie .docx geeft aan dat het om en Microsoft Word bestand gaat in XML-formaat. Zo zijn er vele extensies, we zullen er hier een aantal noemen die je op het systeem regelmatig tegen zult komen:

exe Een executable, dat wil zeggen dat het een commando of een applicatie is die je kan opstarten als je de juiste rechten daarvoor hebt.

log Een log bestand. Bevat informatie over wat er op het systeem gebeurd is.

dll Een dynamic loadable library. Wordt gebruikt door applicaties of commando's.

txt Een text bestand zonder opmaak van de tekst.

ini Een configuratie bestand. Wijzigingen in dit bestand kunnen de manier waarop het systeem werkt veranderen. Met het `type` commando kan je de inhoud van een ini of een txt bestand laten zien op het scherm. Met `notepad` kan je ini en txt bestanden wijzigen.

De `Windows` directory bevat heel veel subdirectories, die gaan we niet allemaal behandelen, maar een paar willen we hier wel benoemen:

\Windows\System32 Bevat executables en libraries die cruciaal zijn voor de werking van het Windows systeem. Hoewel het lijkt of het 32-bits is, wordt de folder gebruikt voor 64-bits zaken.

\Windows\SysWOW64 Een 64-bit operating system kan ook 32-bit applicaties draaien. Op een 64-bit Windows versie vind je de `SysWOW64` folder met daarin de 32-bits files en resources die nodig zijn voor het besturingssysteem. De `SysWOW64` folder is feitelijk de oude `System32` folder met daarin de 32-bits zaken.

6.2 \Program Files

De `Program Files` directory is de plek waar applicaties die niet onderdeel zijn van het besturingssysteem worden geïnstalleerd. Windows 64-bits kan ook Windows 32-bits applicaties draaien. Om deze twee soorten bestanden uit elkaar te houden zijn er op een 64-bits systeem twee `Program Files` directories, een 32-bits Windows systeem kent er maar één.

De applicaties die gebouwd zijn met het aantal bits dat behoort bij het OS worden geïnstalleerd in de `\Program Files`, voor een 32-bits systeem zijn dat de 32-bits applicaties en voor een 64-bits systeem zijn dat de 64-bits applicaties.

De 32-bits applicaties op een 64-bits systeem worden geïnstalleerd in de `\Program Files (x86)` directory. Een 32-bits systeem kent deze directory niet.

6.3 \Users

De `\Users` directory bevat de subdirectories voor alle gebruikers op een systeem. Elke gebruiker heeft zijn eigen directory met daarin zijn of haar documenten.

Index