Hoe veilig is een wachtwoord?

Ton Valkenburgh

We gebruiken natuurlijk allemaal een wachtwoord op onze pc of laptop. De vraag is echter of dat wachtwoord onze gegevens goed beschermt.

Inleiding

Het wachtwoord is de basisbeveiliging op onze pc of laptop. Allemaal vertrouwen we erop dat onze gegevens dus veilig zijn bij bijvoorbeeld diefstal. Wat zijn de mogelijkheden voor een dief om toch bij onze gegevens te komen? Een artikel in de PC-Active 333 laat zien dat het redelijk eenvoudig is om het wachtwoord opnieuw in te stellen, ook als je het oorspronkelijke wachtwoord niet weet. Op de website van de Interessegroep Linux staat ook een tip over hoe je je wachtwoord kunt herstellen als je dat bent vergeten. Kortom, als iemand je laptop in handen krijgt zijn je gegevens, ondanks een wachtwoord, niet veilig.

Een andere manier om toegang tot de harde schijf te verkrijgen is het opstarten van de laptop of pc met Linux vanaf een USB-stick. Daarna kun je bij alle gegevens op een Windows- of Linux-machine. Hoe zorg je nu dat je gegevens wel veilig zijn? Dat kan worden gerealiseerd met een volledige versleuteling van de harde schijf.

De gepubliceerde mogelijkheden om een wachtwoord te resetten waren voor mij de aanzet om toch maar weer versleuteling onder de aandacht te brengen. Het biedt ook de gelegenheid om de informatie te actualiseren.

Versleuteling bij Windows

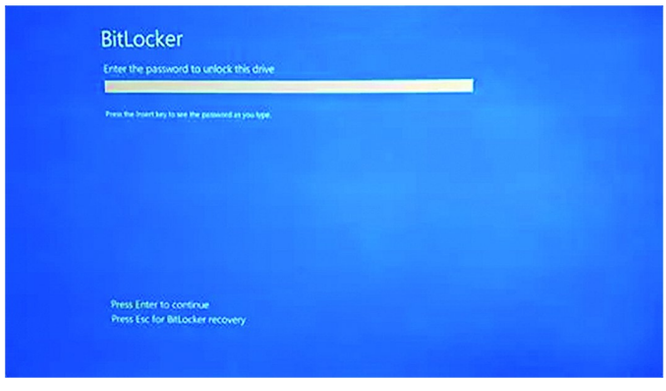
Inderdaad, het versleutelen van je gegevens is de oplossing. De beste aanpak is om de gehele harde schijf te versleutelen. Daar zijn diverse betaalde, maar ook gratis oplossingen voor. Het wachtwoord waar je mee versleutelt, moet je echter niet kwijt raken. Als dat het geval is, kun je niet meer bij je gegevens. Dus berg dat wachtwoord op een veilige plek op.

Juist omdat het niet altijd duidelijk is waar je bestanden worden opgeslagen, is het verstandig de gehele harde schijf te versleutelen. Bij een Windows pc of laptop heb je o.a. de keuze uit: *VeraCrypt*, *DiskCryptor*, *BitLocker* of een *Self Encrypted Drive (SED)*.

VeraCrypt (link 1) en DiskCryptor (link 2) zijn beide open source en het is dus te verifiëren of er geen achterdeurtjes aanwezig zijn. Bij BitLocker moet je Microsoft - als Amerikaans bedrijf - op zijn blauwe ogen vertrouwen. Bij SED's (link 3) ben je ook afhankelijk van de betreffende fabrikant. Als je bescherming wilt hebben tegen willekeurige diefstal en niet van acties door geheime diensten, zou ik kiezen voor VeraCrypt of SED.

VeraCrypt is zeer eenvoudig te installeren. Dat kan ook achteraf zonder dataverlies worden gedaan bij een pc of laptop die al helemaal is geïnstalleerd. VeraCrypt is een software oplossing die uiteraard wel enige belasting geeft. Bij moderne pc's met hardware-encryptie is dat in de praktijk nauwelijks merkbaar. Bij oudere pc's of pc's met een zwakke processor raad ik daarom het gebruik van een SED aan.

BitLocker is standaard aanwezig op Windows Pro, Enterprise en Education. Voor Windows 10 en 11 bestaat er ook apparaatversleuteling. Deze zou automatisch worden geactiveerd als je een Microsoft-account aanmaakt (link 4 en 5). De betreffende pc of laptop moet wel zijn voorzien van TPM en secureboot. Secureboot en DMA-beveiliging moeten zijn ingeschakeld. Bij het activeren van BitLocker wordt automatische een herstelsleutel aangemaakt. Waar deze wordt opgeborgen bepaal je tijdens het activeren.



BitLocker kan ook gebruik maken van de eigenschappen van de SED. Ik heb echter begrepen dat Microsoft hiervan is afgestapt sinds er SED's zijn gesignaleerd die niet goed waren beveiligd.
Een SED is eigenlijk altijd versleuteld. De versleuteling is in de hardware aangebracht. Het maakt niet uit of je de versleuteling gebruikt of niet. De snelheid is in beide gevallen gelijk. Je kunt de versleuteling gebruiken door een wachtwoord aan te brengen. Zolang er na het openen van de SED voedingsspanning op staat, zijn de gegevens beschikbaar. De SED wordt automatisch afgesloten zodra de voedingsspanning wordt verbroken.

Voor SED's is er de industriestandaard TCG/SED. Voor het gebruik van de encryptiemogelijkheid is software van een derde partij nodig. Er is echter ook een open source-oplossing beschikbaar: SEDutil (link 6). *SEDutil* ondersteunt *TCG OPAL 2.00*.

In principe is het mogelijk om een reeds gebruikte SED te versleutelen zonder dat de reeds aanwezige gegevens verloren gaan. Ik heb dat in het verleden zonder problemen gedaan met SED's van Samsung. Later bleek dat niet meer te kunnen bij SED's die ik had gekocht en nog nooit had versleuteld. Ik bleek geen autorisatie te hebben om de SED te versleutelen. De enige mogelijkheid om toch toegang te ver-

krijgen was door een reset van de SED. Daarbij gaan echter wel alle gegevens op de SED verloren. Als je de oude installatie wilt gebruiken zul je eerst een systeemback-up van de SED moeten maken om deze terug te kunnen zetten na het aanbrengen van de versleuteling. CloneZilla (link 7) en RescueZilla (link 8) zijn goede gereedschappen om deze back-up te maken en later terug te zetten.
Als er een aantal SED's in een systeem zitten met hetzelfde wachtwoord, worden deze allemaal geopend door slechts eenmaal het wachtwoord op te geven bij het opstarten.

Versleuteling bij Linux

Ook bij het gebruik van Linux is het mogelijk de harde schijf te versleutelen. Linux heeft standaard *Linux-Unified Key Setup* (link 9) voor versleuteling. Tijdens de installatie van Linux krijg je de mogelijkheid om de harde schijf te versleutelen. Door deze geavanceerde optie te kiezen en het wachtwoord op te geven, wordt de volledige opzet geregeld. Als je Linux zonder deze versleuteling in het verleden hebt geïnstalleerd, kun je de versleuteling helaas niet achteraf aanbrengen. Er zit in dit geval niets anders op dan Linux opnieuw te installeren met de gewenste versleuteling.
Bij Linux met een *Self Encrypted Drive* is het ook mogelijk *SEDutil* te gebruiken. Dat gaat net zo als bij Windows.

Nawoord

Om gegevens die zijn opgeslagen op de harde schijven van een pc of laptop echt te beschermen, is het versleutelen van de harde schijf noodzakelijk. Dit is niet alleen in het belang voor je eigen (bank)gegevens, maar ook bij laptops of pc's die bijvoorbeeld persoonlijke gegevens van leden van een vereniging of andere organisaties bevatten. Hier heb je met de AVG-wetgeving te maken. Als je de machine eenmaal hebt geprepareerd met versleuteling is die na inloggen verder transparant in het gebruik. Daarom hoeft niets je te weerhouden om de beschikbare gratis gereedschappen toe te passen voor deze belangrijke beveiliging. Zie ook een vorig artikel in de SoftwareBus (link 10) voor meer algemene informatie over versleuteling.

Om te zorgen dat het niet zo eenvoudig is om het wachtwoord te kraken, moet het minstens 25 tekens lang zijn. De **lengte** is belangrijker dan de complexiteit van de gebruikte tekens.

Vergeet niet bij het gebruik van versleuteling het wachtwoord veilig op te bergen.
Het is de enige mogelijkheid om bij je versleutelde gegevens te kunnen komen als je het wachtwoord bent vergeten.

Links

1. https://veracrypt.fr/en/Home.html
2. https://diskcryptor.org/
3. https://trustedcomputinggroup.org/resource/self-encrypting-drives-sed-overview/
4. https://www.schoonepc.nl/windows11/windows_apparaatversleuteling_uitschakelen.html
5. https://support.microsoft.com/nl-nl/windows/apparaatversleuteling-in-windows-ad5dcf4b-dbe0-2331-228f-7925c2a3012d
6. https://sedutil.com/
7. https://clonezilla.org/
8. https://rescuezilla.com/
9. https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup
10. https://www.compusers.nl/system/files/swb-jaargangen-leden/2023/2023-2/SwB20232_Encryptie_voor_pc_en_laptop.pdf