Veilig werken?

Ruud Uphoff

Als het niet kan zoals het moet ...
tja, dan moet het maar zoals het kan.

Volkswijsheden worden vaak misbruikt om de grootst mogelijke onzin te bewijzen. Maar soms wijst een gezegde als dit precies de goede kant op! Heel veel veiligheidsadviezen gaan volstrekt voorbij aan de mogelijkheden die de gewone burger heeft. Leuk, al die deskundige taal, maar vertel me iets wat ik daadwerkelijk kan doen, terwijl ik het volledig begrijp. Hoe moeilijk kan het zijn?

Het begon met een mooi artikel in dit blad over de password-manager KeePass. Voor velen interessant en ik gebruik het al jaren. Maar is dat ook een bruikbaar programma voor de doorsnee totaaldigibeet?

Ik heb geprobeerd in mijn omgeving mensen aan te zetten tot gebruik van een password-manager. Vergeefs. Een programma als Keepass is het prototype van software waarmee IT-intelligentsia zich heeft mogen bemoeien.

Je weet wel: het zou mooi zijn als er ook nog een optie zus en een mogelijkheidje zo in gemaakt kon worden.

De instellingen van Keepass zijn niet meer te begrijpen voor een simpele ziel. De opties zijn voor veiligheidsfreaks. Mag dat niet? Jawel hoor, maar de doorsnee gebruiker heeft daar niets aan.

Wat is veiligheid eigenlijk?

Daar kan ik duidelijk over zijn. Veiligheid is een mooi woord voor ‘aanvaardbaar risico’ en als ik iets veilig noem, zwets ik dus uit mijn nek, want ik kan niet bepalen welk risico voor jou aanvaardbaar is. Evenzo de opmerking die iemand maakte over de reden waarom Keepass onveilig was, verwijzend naar de mogelijkheid dat het systeem zou zijn besmet met een keylogger.
De vraag is hier dan ook niet hoe je veilig kunt werken, maar hoe je de gevaren zoveel mogelijk kunt beperken. En als daarvoor geavanceerde mogelijkheden binnen bereik zijn, moet je uiteraard niet nalaten die te gebruiken, maar begin met hetgeen iedereen kan doen.

Veiligheid is een mooi woord voor 'aanvaardbaar risico'.

Wachtwoorden

We weten het nu wel! Wachtwoorden moeten voldoen aan eisen die uitsluiten dat je ze ooit kunt onthouden. Dat kunnen die deskundigen nu wel blijven roepen, maar leg mij nu eens uit hoe iemand in mijn account bij die webshop komt, waar ik als wachtwoord ‘kalepiet’ gebruik. Op een site als deze:

https://howsecureismypassword.net

wordt me verteld dat mijn wachtwoord in vijf seconden gekraakt zou zijn. Nou dat mag je proberen, maar na elke poging krijg je een foutmelding en moet je op OK klikken voor je iets anders kunt proberen. Nog meer onzin om mensen moeilijk te laten werken?
Een zeer voor de hand liggende, maar toch volstrekt onjuiste gedachte, die blijft bestaan als nooit wordt verteld hoe dat kraken wel ongeveer verloopt.

Zo werkt het geboefte niet! Hoe dan wel?

De beheerder van een webwinkel, bank of andere instelling waar we inloggen, weet ons wachtwoord niet. Wachtwoord kwijt? De beheerder kan het je niet vertellen. Het wachtwoord is namelijk vercijferd opgeslagen. En het is niet decodeerbaar, het enige wat het algoritme kan doen is je wachtwoord herkennen: goed of fout. Hoe dat werkt, laten we lekker aan wiskundigen over.

Niet zelden raakt een database met wachtwoorden gecompromitteerd doordat een server kon worden gehackt. Dan beschikt de hacker niet over alle wachtwoorden, maar wel over alle versluierde wachtwoorden. Ik geef je de verzekering dat een wachtwoord van twaalf tekens, zoals dit: **x-TaO13B73OJ** te boek staat als kraakbaar in 34.000 jaar, met andere woorden: dus niet!

Maar hoe verzin je zulke wachtwoorden en hoe kun je ze onthouden?

Twee vragen in één zin en daarop is het antwoord in twee woorden te geven. ‘Niet’ en ‘niet’! Je hebt een eenvoudige wachtwoordgenerator nodig en een wachtwoordbeheerder. Over die laatste kun je net zo moeilijk doen als je wilt, en ja, het kan absoluut veiliger dan ik nu ga vertellen, maar als je niet overweg kunt met al het aanbevolen spul, gebruik dan wat je standaard al ter beschikking hebt: je browser! Ik hoor meteen al het geroep: ‘Dat is onveilig!’ O ja? Wat is het risico?

Wachtwoorden, steeds maar weer die wachtwoorden.

Die risico’s zijn er inderdaad, maar met risico’s kun je leren omgaan. Autorijden is ook levensgevaarlijk, en daarom laten we mensen dan ook een rijbewijs halen! Je smartphone in de auto is ook levensgevaarlijk, maar dat gevaar verdwijnt als je ’m gewoon niet gebruikt. En zo kun je ook met de opgeslagen wachtwoorden in je browser veilig omgaan.

Hoe (on)veilig zijn wachtwoorden, opgeslagen in de browser?

Het gebruik van een password-manager heeft nog steeds de voorkeur, maar als de installatie en het gebruik daarvan voor

de gebruiker te ingewikkeld is, moet dat geen reden zijn om dan maar weer gemakkelijk te onthouden (en te kraken) wachtwoorden te gebruiken, liefst op meerdere plaatsen hetzelfde.

De voorzieningen in de browser zijn simpel door iedereen te gebruiken. Als je eenmaal ergens bent ingelogd, met een zojuist aangemaakt onmogelijk te onthouden wachtwoord, vraagt de browser of het wachtwoord moet worden opgeslagen. Je hoeft alleen maar op 'ja' te klikken.

Alle vier de hier genoemde browsers geven je ook de mogelijkheid de opgeslagen wachtwoorden met elke andere computer te synchroniseren. Dat gebeurt met Edge en IE door onder Windows 10 je instellingen te synchroniseren.

- **Windows 10**
(Edge, Internet Explorer)
Ga naar *Startknop → Instellingen → Accounts → Uw instellingen synchroniseren* en zet de schakelaar bij *Wachtwoorden* aan.

- **Chrome**
Ga in het menu van de drie puntjes, rechts bovenaan, naar *Instellingen → Personen*. Als daar de naam van je Google-account nog niet staat, kies dan voor *AANMELDEN BIJ CHROME* en vul je Google-account in. Kies dan voor Synchronisatie en zet minimaal de schakelaar *Wachtwoorden* aan.

- **Firefox**
Ga naar *Extra → Opties Firefox-account*. Kies, indien nog niet gedaan, *Account aanmaken*. Hierna kun je Firefox synchroniseren met andere apparaten. Firefox biedt ook nog de mogelijkheid opgeslagen wachtwoorden met een extra wachtwoord te beveiligen.
Niet nodig als geen anderen toegang hebben tot je account.

Je wachtwoorden staan nu in de cloud. Google Chrome geeft je toegang tot je wachtwoorden vanaf elk ander apparaat als je gaat naar **http://passwords.google.com** en inlogt met je Google-account.
Wat nu als de site van Google wordt gehackt? Dan nóg hebben de boeven je Google-password nodig om je wachtwoorden te kunnen ontcijferen.

Maar hoe maak je even een sterk wachtwoord?

Eenvoudig: daar zijn wachtwoordgenerators voor.
Ik heb er ooit zelf een geschreven, met als uitgangspunt dat het kinderlijk eenvoudig moet zijn.

Download **https://www.uphoff.eu/files/pwgen.zip** en pak de twee bestandjes uit in een map naar keuze met een naam naar keuze.

Als je het *progje* start, met een muisklik, opent het kladblok met twintig unieke sterke wachtwoorden van 12 tekens in het bestand ***pass20.txt*** dat in dezelfde map komt te staan.
Wie nog meer wil kan het **ini**-bestandje in dezelfde map bewerken.