Improve: Persoonlijke Veiligheid

Thema 1: Password Manager

Ik wil om te beginnen even kijken naar mijn wachtwoorden en hoe ik deze op een beter en veiligere manier kan opslaan.

Tot op heden gebruik ik Google Chrome om mijn wachtwoorden op te slaan. Na de lessen over encryptie en decryptie heb ik wat onderzoek gedaan naar hoe Chrome mijn wachtwoorden opslaat en was in shock om te lezen dat deze werden opgeslagen in “plain text”.

Daarom heb ik ervoor gekozen om te migreren naar Bitwarden. Deze is een gratis en open-source service, die tot op heden nog niet gehackt is geweest. Ook maakt ze gebruik van AES-256 encryptie. Dit betekent kortom dat er een sleutel gebruikt wordt die 256 bits in lengte is om de data zowel te encrypteren als decrypteren.

Om mijn data te migreren naar Bitwarden heb ik gebruik gemaakt van deze stappen. Hierin staat duidelijk vermeld wat de stappen zijn om alles te migreren.

Ten slotte heb ik dan mijn al mijn wachtwoorden Chrome verwijderd en ingesteld om mij niet meer te vragen om een wachtwoord op Chrome op te slaan. Op deze manier loop ik geen risico meer en worden mijn wachtwoorden op een veilige manier opgeslagen.

Services zoals LastPass en Bitwarden helpen je niet alleen met het opslaan van je wachtwoorden, maar ook met het aanmaken ervan. Bij het aanmaken van een nieuw account op eender welke website kan je een sterk wachtwoord genereren en gebruiken. Dit zorgt er dus voor dat je niet meerdere wachtwoorden gaat gebruiken voor meerdere websites, wat zeer onveilig is.

Thema 2: Back-ups

Vervolgens wil ik het hebben over mijn persoonlijke data, namelijk mijn muziek, foto’s en media, maar ook mijn afgeronde opdrachten op de hogeschool. Deze worden nog altijd, buiten mijn media (TV Series, Films, …), op de klassieke manier opgeslagen, op 1 pc en op 1 locatie. Wat maakt dat ik een groot risico loop op dataverlies. Als de schijf waar al mijn data opstaat faalt, verlies ik zomaar al mijn data.

Om dit tegen te gaan voer ik de 3-2-1 regel toe. 3 kopieën van je data, waaronder 1 originele en 2 kopieën. Opgeslagen op 2 verschillende apparaten/mediums. Met 1 kopie off-site. Om dit te behalen kies ik ervoor om ook al mijn foto’s, muziek en schoolopdrachten op mijn homeserver op te slaan. Hier stond mijn media al op (deze wordt namelijk via Plex gedeeld over het netwerk). Om dit alles niet elke keer handmatig te moeten overzetten, heeft Windows een gestroomlijnde manier om dit te

automatiseren. Via de optie “Update & Security” in de instellingen kan je kiezen om en back-up op te slaan naar een netwerklocatie en dit kan je dan ook nog eens automatiseren om bijvoorbeeld elke week 1 keer uit te voeren. Voor een meer uitgebreide uitleg kan je hier de stappen vinden die ik heb geraadpleegd.

Ook op mijn server, heb ik een vorm van redundantie. Ik maak namelijk gebruik van Raid 1. Dit wil zeggen dat als een van de 2 schijven in mijn server faalt, ik de data niet verlies.

Dit alles zorgt ervoor dat ik dus al een 2de kopie heb, meteen ook al op een 2de medium. Om nog te voldoen aan de laatste regel heb ik een off-site oplossing nodig. Hiervoor ga ik gebruik maken van Google Drive.

Google biedt gratis voor iedereen 15GB aan opslag aan. Dit is niet genoeg voor de enorme bibliotheek aan muziek en series die ik in mijn bezitting heb en zal daarom deze niet mee kunnen opslaan op de off-site locatie, maar is voorlopig een risico dat ik zal moeten nemen tot ik een andere off-site oplossing heb gevonden.

Ten slotte betekent dit nu dat als mijn pc faalt, ik al mijn data nog kan herstellen van mijn server. In de server kan er een van de schijven falen voor ik data verlies. En moest deze ook nog falen, dan kan ik de belangrijkste bestanden nog terugvinden op mijn Google Drive.

Thema 3: Have I Been Pwned

Als laatste heb ik gekozen om te kijken welke platformen er data van mij hebben dat gebreached is geweest. Om dit na te kijken kan je een website raadplegen: Have I Been Pwned?. Hier geef je je email in en vervolgens laat ze zien welke platformen er in het verleden gebreached werden, waar jij een account op hebt. Ze laat zien welke websites er gebreached werden, maar ook wat voor soort data er gecomprimeerd werd. Zeker in de hedendaagse maatschappij is het zeker geen slecht idee om regelmatig deze website te checken.

Na zo een databreach bevinden je wachtwoorden en emailadressen zich openbaar op het internet. Dit is een serieus risico.

Om de breaches tegen te gaan heb ik al de wachtwoorden van de gebreachte websites verandert, samen met de usernames waar mogelijk. Voor de meeste is dit echter niet genoeg. Als je namelijk nog geen paswoordmanager gebruikt en je hetzelfde wachtwoord op meerdere websites, dan pas je deze ook best aan. Om helemaal zeker te zijn heb ik al de wachtwoorden verandert van de accounts die ik voor de laatste breach heb aangemaakt.