Improve: Veiligheidsvoorschriften

Inleiding

In deze opdracht kies ik een cloudopslagplatform als IoT-project. Verder ga ik in dit verslag de veiligheidsrisico's bespreken en onder de loep nemen. Met als kader het gebruiken van een online cloudopslagplatform zoals Google Drive of Apple iCloud.

Risico's

Om te beginnen is het geen slecht idee om een sterk wachtwoord of wachtwoordzin te kiezen om passwoord inbreuken te voorkomen. Het kan hier best handig zijn om een passwoordmanager zoals lastpass of bitwarden. Deze helpen bij het aanmaken van een sterk en lang wachtwoord elke keer dat je ergens een account aanmaakt. Daarna kan je bij elke login het wachtwoord simpelweg aanklikken. Belangrijk is hier wel dat je je hoofdwachtwoord, of idealiter wachtwoordzin, op een veilige manier opslaat. Activeren van two-factor authenticatie is hier ook zeker geen slecht idee om ongeautoriseerde toegang tegen te gaan.

Vervolgens moeten we ook rekening houden met het verlies van data. Cloud platform providers hebben normaalgezien een robuust back-up systeem, toch is er nog steeds risico dat er data verloren gaat. Dit door hardware dat faalt, software bugs of andere technische fouten. Om dit te voorkomen kan je je best houden aan wat ze de 3-2-1 regel noemen. Dit houdt in, 3 kopieën van je data (waaronder het origineel en 2 kopieën) op 2 verschillende medium met 1 kopie die zich off-site begeeft.

Je houdt dus best nog een kopie van de data bij op een ander medium lokaal bij je thuis en om helemaal safe te zijn, een kopie buitenshuis.

Verder moeten we ons ook zorgen maken over het privacy-aspect. Het gebruiken van een cloudopslagplatform betekent namelijk ook dat je wat controle over de privacy afgeeft. Je moet ervan uitgaan dat de providers van het cloudplatform hun beleid nakomen met betrekking tot de privacy. Er bestaat ook het risico van ongeautoriseerde toegang tot jouw gevoelige informatie.

Om je hierop voor te bereiden lees je best de gehele gebruiksvoorwaarden aandachtig door en beslis je op basis daarvan welke provider het best past bij jou noden.

Een ander risico kunnen data breaches zijn. Cloudopslagplatformen zijn een primair doelwit voor cybercriminelen dankzij de grote hoeveelheid aan data dat ze bijhouden. Als de security van deze providers doorbroken wordt, kan er veel sensitieve data gecompromitteerd worden.

Om te voorkomen dat jouw sensitieve data zomaar de wijde wereld terecht in komt, kan je ervoor kiezen om ze te encrypteren voordat je ze opslaat in de Cloud. Op deze manier ben je de hackers een stapje voor moesten ze erin slagen om de robuuste veiligheidsmaatregelen van je provider te kraken.

Ten slotte komen er ook nog risico's kijken bij het delen van folders of bestanden op een cloudplatform. Bij bijvoorbeeld Google Drive kan je bestanden en folders delen via een link. Deze link kan misbruikt worden als de verkeerde persoon ze te pakken krijgt.

Daarom kan je best de permissies van z'n link aanpassen naar de noden van de ontvanger. Je geeft dus geen toegang tot alle folders als ze maar een specifiek bestand nodig hebben. Ook is het een goede gewoonte om regelmatig te checken of bestanden niet bekeken en/of aangepast worden door onbekende gebruikers.

Slot

Het gebruiken van een cloudopslagplatform als Google Drive komt met vele voordelen zoals gemakkelijk in gebruik te nemen, eenvoudig om met andere samen te werken en file versioncontrol zoals Git. Toch is het belangrijk om bovenstaande risico's in acht te nemen voor je een beslissing maakt.