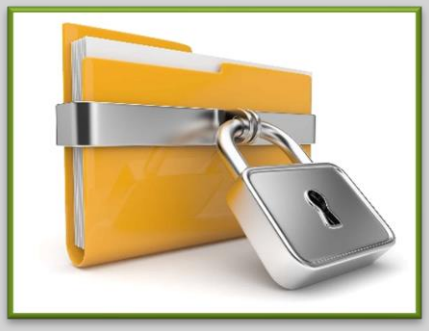
Cybersecurity in het Smart Energie project.

In dit project werk ik met data afkomstig van de “smart meters” die aangesloten zijn op meterkasten, deze meters sturen data door naar een database die aangeeft hoeveel energie en gas er gebruikt word in een huishouden. Deze data word gebruikt om bijvoorbeeld alles weer te geven met grafieken op een webpagina. Het cybersecurity gedeelte van dit project is natuurlijk extreem belangrijk omdat we werken met gegevens van huishoudens, oftewel privacygevoelige informatie. Het is daarom cruciaal om potentiële risico’s te vinden en te zorgen dat er geen misbruik van gemaakt kan worden om deze gevoelige informatie te beschermen.

De risico’s

Een van de grootste risico’s in dit project is phishing. We werken met gegevens die verbonden zijn aan gebruikers en huishoudens. Deze informatie is gevoelig omdat het veel kan aantonen, zo kun je zien wanneer iemand bijvoorbeeld voor een lange tijd niet thuis is omdat het gas en energie verbruik weinig tot niks is. Ook andere vormen van datadiefstal en ransomware-aanvallen zijn een serieus gevaar. Als iemand zoals bijvoorbeeld een crimineel het voor elkaar heeft om toegang te krijgen tot alle data, kunnen ze deze stelen of versleutelen om bijvoorbeeld geld te eisen voor deze gegevens. Dit kan leiden tot verlies van gegevens maar ook het vertrouwen wat de gebruikers in het project hebben. Ook een risico zijn DDoS-aanvallen en SQL-injecties, een DDoS-aanval kan zorgen voor een systeemuitval en downtime.



Privacygevoelige gegevens beschermen

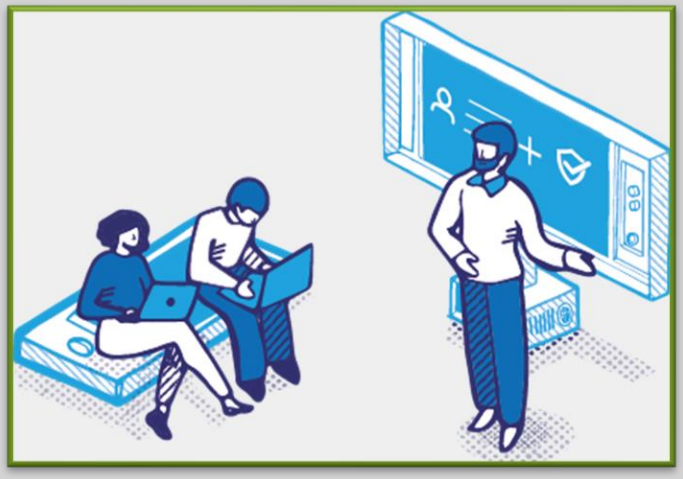
Slimme meters verzamelen heel veel data, veel is mogelijk privacygevoelig. Denk aan het energie en gasverbruik zoals eerder genoemd, onwaarschijnlijk omdat gegevens geanonimiseerd zijn(het kan niet gelinkt worden aan een persoon of huishouden, de metingen zijn anoniem), maar ook persoonlijke gegevens zoals namen en adressen. Deze gegevens kunnen zeer waardevol zijn. Daarom moet deze informatie goed beschermd worden met de juiste beveiligingsmaatregelen.

Beveiligingsmaatregelen

Om de net benoemde risico's te beperken, zorg ik dat er verschillende maatregelen in het project komen. Op het moment is het project nog alleen lokaal, maar als deze uiteindelijk online komt moet er gezorgd worden voor een goed login systeem met een multifactorauthenticatie (MFA), zo heb je meer zekerheid over wie wel en niet de gegevens kan zien en voorkom je ongeautoriseerde toegang. MFA zorgt er voor dat gebruikers ook na het inloggen nog een extra stap moeten maken, dat kan bijvoorbeeld een SMS-code zijn, of een biometrische verificatie zoals gezichtsherkenning, pas als ze voldoen aan deze stappen mogen ze het systeem in.

Ook is het enorm belangrijk om de geschreven software regelmatig te updaten zodat er geen misbruik gemaakt kan worden van potentiële beveiligingslekken. De gebruikers bewust maken van problemen zoals phishing is ook enorm belangrijk, daarnaast helpt een strengere wachtwoordeis ook met het beveiligen van accounts als de eventuele inlog er eenmaal in zit.

Zo kunnen gebruikers zelf ook actief helpen bij het beveiligen van hun gegevens.



Conclusie

Cybersecurity is enorm belangrijk bij projecten zoals deze, de risico's van cyberaanvallen kunnen grote gevolgen hebben als er niks aan gedaan word. Door gebruik te maken van alle benoemde maatregelen en de gebruikers te informeren over de gevaren en hun bewust te maken van hoe belangrijk het is om veilig om te gaan met gegevens hoop ik dat het project en de algemene veiligheid online een stukje beter word.

Zo behouden we ook het vertrouwen van de gebruikers in het project.