Kwaadaardig internet onderscheppen

Voor dit project wordt er eerst een theoretisch onderzoek gedaan als voorstudie voor het ontwikkelen van een software firewall. De software wordt ontwikkeld in Python. Het project is bedoeld om een beter inzicht te verkrijgen in de werking van malware.   
  
Malware is een samentrekking van het Engelse woord malicious software en wordt vertaald als kwaadaardig en schadelijke software. Het vormt een dagelijkse dreiging voor het internet verkeer en kent vele vormen. Vanuit de vraag naar bescherming zal er worden gezocht naar een mogelijke oplossing vanuit het inzicht dat in de voorstudie werd verkregen. Dergelijke oplossingen bestaan reeds en worden door verschillende software bedrijven op de markt gebracht. Het is dan ook niet de kern van dit project om een betere oplossing te bekomen, maar om een ruimer inzicht in een deelaspect van computerbeveiliging te krijgen.   
  
In het eerste hoofdstuk wordt onderzocht wat malware is. In deze studie zal besproken worden welke types er bestaan en wat voor effecten deze hebben bij het geïnfecteerde toestel.  
  
Vervolgens worden de bestaande oplossingen besproken. Dit hoofdstuk behandeld firewalls en antivirussoftware.   
  
Uit al deze voorgaande kennis zal in het volgende hoofdstukken een mogelijke oplossing worden voorgesteld. Het behandeld de software firewall die ontwikkeld wordt in Python. Het filteren en analyseren van netwerk pakketten zal plaatsvinden op netwerk laag drie en netwerk laag vier. Netwerk pakketten uit landen die een verhoogd risico vormen kunnen door de ingebouwde geolocatie worden geblokkeerd. De software draait op een centrale server die samen fungeert met de firewall software. Hierdoor kan deze ook fungeren als een man in the middle. Dit is nodig om HTTPS pakketten te decrypteren. De firewall zal ook vroegtijdig een Denial of Service aanval kunnen detecteren en stoppen. Er is interactie tussen de firewall en de eindgebruiker, zodat deze steeds op de hoogte wordt gesteld van mogelijke aanvallen. De gebruiksvriendelijke interface biedt een eenvoudig beheer. Ten slotte volgt een voorstel tot een mogelijk vervolg waar wordt besproken of artificiële intelligentie en rol zou kunnen spelen bij de behandeling van netwerk pakketten.   
  
De belangrijkste onderzoeksmethode is literatuurstudie van online bronnen. Het geeft inzicht in de werking van malware en hoe er zich tegen te beschermen. Ook geven de vele testen die worden uitgevoerd op de firewall bij de ontwikkeling ervan vele inzichten. De interface wordt geëvalueerd door middel van gebruikerstesten, ze worden op regelmatige tijdstippen in het proces voorgelegd.