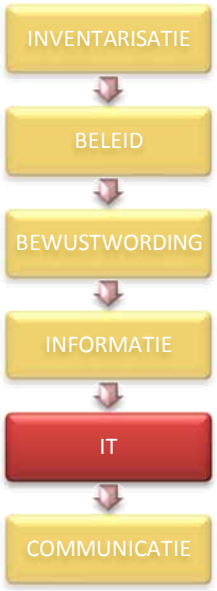
5.2 TOETSEN

Doelstelling: *Het, met behulp van externe 'aanvallen', in kaart brengen van de zwakke plekken binnen de ICT beveiliging en een aanbeveling opstellen voor verbetering.*



Ethisch hacken brengt zwakke plekken in de ICT beveiliging op een integere manier aan het licht.
Door met regelmaat de eigen beveiliging te toetsen groeit het vertrouwen in de weerbaarheid van de onderneming. Door de snelheid waarmee technieken zich ontwikkelen is het bijna ondoenlijk om ook de bijkomende vormen van fraude tegen te gaan.
De fysieke beveiliging van de infrastructuur, de soft- en hardware, de procesmatige beveiliging en de rol van de mens in dat proces kunnen m.b.v. ethisch hacken of door social engineering worden getoetst.

Case:

Tijdens een eerdere audit had organisatie X een ethische hack aanval op haar infrastructuur laten uitvoeren. Gelukkig kwamen hier geen opmerkelijke issues uit naar voren. Wat wel opmerkelijk was, was de behulpzaamheid van medewerkers om e.e.a. mogelijk te maken. Reden voor het management om deze behulpzaamheid ook te toetsen bij de afgifte van wachtwoorden.

Oplossing:

Door middel van Social Engineering heeft TRES PRETIA® zowel telefonisch als in de persoon van een Mystery Guest getracht een aantal wachtwoorden van medewerkers los te krijgen.
Door het simuleren van een situatie waarbij hun hulp werd vereist, kregen we veel meer informatie dan nodig was en eigenlijk voor mogelijk gehouden werd.
Hiermee werd de dienstbaarheid in strijd met veiligheid aangetoond.
TRES PRETIA® heeft vervolgens het beleid hierop aangepast door het aantal mensen dat informatie over de infrastructuur mag afgeven, te beperken.
Tevens is tijdens een bewustwordingsprogramma het principe 'nice to know' en 'need to know' nader toegelicht.