Abstract

"Social engineering: de menselijke schakel in de informatiebeveiliging"

Voor bedrijven en de overheid is het belangrijk dat gevoelige en geheime informatie niet in verkeerde handen zal vallen. Met de huidige stand van de techniek wordt het steeds moeilijker om deze informatie te beschermen als gevolg van de hogere connectiviteit. Bedrijven en overheden zijn aangesloten op het World Wide Web en daarmee zijn ze verbonden met de hele wereld. Er zijn tal van gespecialiseerde bedrijven die zich bezig houden met het beveiligen van informatie. Deze bedrijven bieden vaak technische oplossingen die ongewenste toegang tot informatie kunnen voorkomen. Echter niet alle beveiligingsproblemen kunnen opgelost worden met geavanceerde technologieën omdat de **mens** ook nog altijd een rol zal spelen. Een systeem kan waterdicht beveiligd zijn, maar er zullen altijd mensen toegang hebben tot dit systeem. De menselijke factor wordt vaak gezien als "de zwakste schakel in de informatiebeveiliging" omdat mensen goedgelovig, ongeïnformeerd, goed van vertrouwen en behulpzaam zijn. De techniek waarbij dankbaar gebruik wordt gemaakt van deze zwakheden van de mens wordt: "Social Engineering" genoemd. Social engineering kan omschreven worden als "door hackers gebruikte psychologische trucs met als doel het verkrijgen van gevoelige informatie om toegang te krijgen tot beveiligde systemen".

In dit onderzoek worden manieren gezocht waarmee bedrijven een social engineeraanval kunnen **voorkomen** of zich kunnen **wapenen** tegen een aanval.

Door te kijken naar de verschillende drijfveren achter social engineering worden manieren onderzocht om te voorkomen dat een bedrijf doelwit wordt van een social engineeringpoging. Het resultaat hiervan is een **kwetsbaar bedrijfsprofiel**. Als bedrijven hieraan voldoen zullen ze een verhoogd risico op een aanval lopen en is het verstandig dat deze bedrijven maatregelen treffen.

Er wordt ook gekeken naar hoe een social engineeraanval in elkaar steekt. Binnen een social engineeraanval is het van belang dat de social engineer stukje bij beetje **informatie** inwint over het bedrijf. Doordat de social engineer steeds meer informatie over het bedrijf in zijn bezit heeft komt kan hij geloofwaardig overkomen en weet hij waar en bij wie hij moet zijn binnen het bedrijf. Hij komt stap voor stap dichter bij zijn einddoel. Het uiteindelijke einddoel zal bestaan uit het inwinnen van bedrijfsgeheimen uit informatiesystemen.
Tijdens het onderzoek zijn de informatiestromen in kaart gebracht en is gekeken naar de "bottleneck" binnen het informatie inwinproces. Bedrijven kunnen zich wapenen tegen social engineering door deze bottleneck te **beveiligen**. Als de bottleneck eenmaal beveiligd is zal een social engineeraanval op dit punt stuk lopen en wordt het einddoel dus niet bereikt.

Dit onderzoek is uitgevoerd aan de Radboud Universiteit te Nijmegen in het kader van de Master scriptie van de opleiding Informatiekunde. Het onderzoek is begeleid door dr. L. Consoli en dr. P. van Bommel.

Dick Janssen, november 2005