HET GEBRUIK VAN SOCIAL ENGINEERING EN SOCIALE MEDIA DOOR HACKERS

Dr. Elly Broos, Nederlandse Defensie Academie

Dr. Elly Broos is als universitair docent Human Resource Management en onderzoeker verbonden aan de Faculteit Militaire Wetenschappen van de Nederlandse Defensie Academie. In dit artikel gaat dr. Elly Broos nader in op het gebruik van *social engineering* en sociale media door hackers. Hierbij wordt haarfijn uit de doeken gedaan hoe hackers, cyber booswichten, doordacht gebruik maken van beïnvloedingstactieken. Herken een aanval en word weerbaar.

HACKERSAANVAL

In november dit jaar, heeft Defensie last gehad van een nieuw e-mail virus. Het virus wordt inmiddels geblokkeerd door het systeem, maar IVENT waarschuwt om niet op de gevoegde hyperlink in de e-mail te klikken en deze e-mail te verwijderen. De inhoud van de mail, ziet er ongeveer als volgt uit: *"Hallo ****@mindef.nl, Thank you for the order. Your credit card will be charged for 330 dollars. For more information, please visit our website".*

Dit is een typisch voorbeeld van een hackersaanval, waarbij het doelwit een grote groep ICT gebruikers is, die onder valse voorwendselen verleid worden, om op een hyperlink of URL in de e-mail te klikken of een document te openen. Hierdoor kan een virus of malware op het netwerk komen en zich verder verspreiden. Het is soms makkelijker en meer productief om via mensen het systeem binnen te komen, dan via een technische *vulnerability*. De motieven van hackers zijn uiteenlopend. In dit geval kan het bericht afkomstig zijn van een cybercrimineel of een cyberspion. Het is echter ook mogelijk dat dit bericht onderdeel is van een geplande cyberaanval door een groepering specifiek gericht op de Defensiesystemen.

SOCIAL ENGINEERING

In de boodschap van deze e-mail zijn er bepaalde beïnvloedingstechnieken waar te nemen, waardoor er gepoogd wordt de lezer van de e-mail op de gevoegde link te laten klikken, mede door bepaalde prikkels te activeren waarop mensen vaak onbewust reageren. Het beïnvloeden en manipuleren van mensen om hun gedrag te beïnvloeden, wordt ook wel *social engineering* genoemd. Dit is bijvoorbeeld terug te zien in marketing om het koopgedrag van consumenten te beïnvloeden. Echter, in toenemende mate wordt *social engineering* ook gebruikt door computerkrakers, met het uiteindelijke doel om via mensen in systemen of netwerken te infiltreren. Dit kan via e-mail, een nepsite, maar ook via telefonisch of direct contact met een gebruiker van een systeem. Het doel van dit artikel is om een aantal van deze beïnvloedingstactieken in kaart te brengen. Verder worden de risico's van misbruik van informatie op sociale media, zoals Facebook, LinkedIn en Twitter, door computerkrakers in de voorbereidende fase van een doelgerichte aanval op een systeem via een bepaalde persoon of personen, toegelicht.

BEÏNVLOEDINGSPRINCIPES

In bovenstaand mailtje zijn een aantal typische social engineering principes terug te zien.
Een boodschap bevat naast het zakelijke aspect doorgaans ook een appellerend aspect dat de ontvanger aanspoort actie te ondernemen, zoals het lezen van een document, het antwoorden van een vraag of een bepaalde gedraging, zoals het geven van informatie. Gedragingen van mensen worden deels cognitief bepaald, bijvoorbeeld door het afwegen van verschillende opties, of het nadenken over risico's. Echter, over veel handelingen denken mensen niet bewust na en wordt het gedrag op een onbewust vlak bepaald.
Zo roept: *'Thank you for the order'* emotie op, bijvoorbeeld verontwaardiging of verbazing. Impliciet ontstaat de vraag – heb ik een order geplaatst? Mensen ervaren doorgaans een prikkel om te antwoorden op een vraag en hierdoor is de aandacht op de inhoud van de mail gevestigd.
Dit leidt af van andere zaken, zoals het nadenken over het risico van virussen en malware gelinkt met spam-mail of in dit voorbeeld, de ongebruikelijke adressering. Een emotie van verontwaardiging wordt geprikkeld omdat er genoemd wordt dat er een bedrag van de creditcard wordt afgeschreven.
De dreiging dat er geld wordt afgeschreven, roept emotie van machteloosheid op, waardoor je zo gauw als mogelijk actie wilt ondernemen en zo is de lezer beïnvloed om de link te willen aanklikken om meer informatie en uiteindelijk beheer te krijgen over de situatie. Dit wordt verder versterkt door het tijdsaspect 'binnenkort'. Een tijdsindicatie heeft het psychologische effect dat een gevoel van urgentie ontstaat.

Samenvattend zien we de volgende beïnvloedingsprincipes terug:
- het oproepen van emotie,
- het (impliciet) stellen van een vraag,
- het creëren van urgentie om actie te ondernemen.

Deze prikkels appelleren vaak aan het onbewust gedrag van mensen. Soortelijke e-mails worden aan een wijd publiek verzonden en nep-websites en pop-ups moedigen Internet gebruikers om een gecompromitteerde link aan te klikken, waardoor malware op het systeem wordt geïnstalleerd.

INFILTRATIE: STAP VOOR STAP

Het is echter ook mogelijk dat een doelgerichte aanval wordt uitgevoerd door computerkrakers, waarbij één of meerdere individuen worden geïdentificeerd die toegang hebben of deel zijn van een organisatie, waarbij het uiteindelijke doel een geplande infiltratie in de systemen is. Dit kan bijvoorbeeld het achterhalen van een gebruikersnaam en wachtwoord van een systeemadministrator zijn, omdat dit het mogelijk maakt dieper in het systeem te komen voor een volgende stap.

Een gerichte aanval op een systeem, wordt zorgvuldig voorbereid. Er kunnen hierin een aantal fasen worden onderscheiden.
- Eerst worden algemene inlichtingen verzameld, bijvoorbeeld via het Internet of via sociale media, over de organisatie en de informatiesystemen.
- Daarna worden belangrijke sleutelpersonen geïdentificeerd.
- De volgende stap is het verzamelen van zoveel als mogelijk informatie over deze personen en de systemen, bijvoorbeeld waar de belangrijke servers staan en

welke software wordt gebruikt, contactgegevens, maar ook over wie welke rol vervuld in de organisatie en geaffilieerde bedrijven.

Dit wordt vaak stapsgewijs uitgevoerd en op diverse manieren.

Sociale media kunnen in deze fase een belangrijke rol spelen. Een groot percentage ICT gebruikers kiest nog steeds wachtwoorden zoals '12345', voornamen, achternamen en 'qwerty' als er geen regels worden opgelegd voor een bepaalde lengte en combinaties letters, getallen en punctuatie. Sociale engineers kunnen soms via een paar raadpogingen of met behulp van een speciale applicatie, toegang krijgen tot een bestaand profiel van een doelwit en kunnen hierdoor nog dieper zoeken in de informatie of zich voordoen als de eigenaar van het profiel en vervolgens nog wat informatie opvragen bij vrienden of kennissen van het profiel.

Er zijn diverse tools beschikbaar om de gevonden informatie op te slaan in een speciale database, waarin geautomatiseerd verbanden kunnen worden gezocht tussen stukjes informatie en waarbij de informatie wordt gecategoriseerd en geordend en het inzichtelijk wordt welke informatie nog nodig is om een gerichte aanval te beginnen. Er zijn ook gespecialiseerde zoekapplicaties voor potentiële computerkrakers, waarmee op het Internet en via sociale media informatie over een specifiek persoon of organisatie bijeen kan worden gebracht. Zodra voldoende informatie is verzameld, kan er een gerichte hackingsaanval plaatsvinden. Dit kan via een gerichte e-mail of nepsite, maar dit kan ook via de telefoon of via directe toegang. De hackingsaanval via de telefoon wordt geloofwaardiger als via spoofing technologie het telefoonnummer dat bij de gespeelde rol en context past, wordt getoond. Vervolgens kan onder valse voorwendselen informatie, zoals specificatie van de software of de locatie van servers worden opgevraagd. Soms wordt telefonisch aangekondigd dat er een belangrijk bericht via de mail is verstuurd, waarna de kans aanzienlijk wordt vergroot dat de medewerker het document opent.

Het is echter ook mogelijk dat een computerkraker een deel van de aanval via direct contact laat plaatsvinden. Door een geloofwaardige context te creëren waarin de computerkraker een passende rol speelt, kan een medewerker soms worden overgehaald om een gegevensdrager zoals een usb-stick in het systeem te plaatsen, bijvoorbeeld onder het voorwendsel dat de computerkraker documenten is vergeten uit te printen of er koffie over de documenten is gemorst. De geloofwaardigheid van de computerkraker neemt toe als hij/zij een aantal feiten weet te noemen die kloppen, bijvoorbeeld namen, functies en afspraken van andere medewerkers bij de organisatie. Sociale media maakt het makkelijker om deze informatie te vinden. Met de juiste informatie en houding kan de computerkraker het vertrouwen van een medewerker winnen om toegang te krijgen tot een kantoor of tot een systeem, of nog een stuk ontbrekende informatie. Soms vinden er gefaseerd meerdere aanvallen plaats om het uiteindelijke doel te bereiken.
Informatie vanaf sociale media wordt in toenemende mate gebruikt. Informatie op zichzelf lijkt misschien onbelangrijk, maar het kan een puzzelstuk zijn in een groter geheel. De voornemende infiltrant heeft de uitdaging om de stukjes informatie te vinden en in elkaar te passen. Dit gedeelte kan ook worden uitbesteed bij professionele informatiebrokers. Allerlei middelen kunnen worden ingezet en toepasselijke informatie kan via sociale media ook in de directe vrienden/kennissenomgeving worden gezocht.

Het bestaan van een moeizame financiële situatie, vrienden of familieleden met verslavingsproblemen, kinderen op onlinegaming sites kunnen worden misbruikt om informatie in te winnen of zelfs om ID fraude te plegen. Niemand wordt ontzien en hierbij zijn ethische normen ver te zoeken.

Een opportunistisch voorbeeld is dat, na een grootschalige ramp waarbij mensen vermist zijn, er soms professioneel uitziende nep-websites worden gemaakt, waarbij de indruk wordt gewekt dat familieleden en vrienden informatie over hun vermisten kunnen krijgen, mits ze een formulier invullen waarbij allerlei gevoelige informatie wordt gevraagd. De sterke emotie (begeerte om iets over de vermiste vriend of het familielid te horen) overstemt de intuïtie van gevaar en informatie wordt makkelijk gegeven. Bij computerkrakers met criminele motieven, is financieel gewin meestal de drijfveer, maar het komt bijvoorbeeld ook voor dat organisaties concurrenten willen benadelen door een netwerk gedeeltelijk uit te schakelen of wederrechtelijk bedrijfsinformatie in te zien.

Een gevoel van verbondenheid en vertrouwen komt sneller tot stand als er een gemeenschappelijke belangstelling is tussen mensen. Via sociale media wordt vaak duidelijk wat belangrijk is voor iemand en wat de specifieke interesses zijn. Een onbekende met dezelfde interesses of ideologieën kan via wat voorwerk een geloofwaardige context creëren en een kennis worden via sociale media. Zodra er een vertrouwensband is gevestigd, kan de computerkraker het wederkerigheidsprincipe toepassen. De computerkraker biedt iets aan dat te maken heeft met de gemeenschappelijke belangstelling (bijvoorbeeld als de 'gedeelde' belangstelling legomodellen is, kan een document met legomodellen worden gestuurd of als iemand een baan zoekt, kan een valse, maar passende vacature worden aangeboden. Vervolgens ontstaat een behoefte bij de ontvanger om iets terug te doen, nl het klikken op de link. Als de gebruiker geen afdoende anti-spy of malware programma heeft, is het systeem gecompromitteerd. Via malware kunnen bijvoorbeeld inloggegevens worden gelogd, maar er kan ook op afstand in het systeem worden gezocht naar ontbrekende stukken informatie. Uiteraard gebeurt dit bij voorkeur op momenten dat de gebruiker niet bezig is op het systeem.

In de tabel op de volgende bladzijde worden een aantal psychologische en sociologische eigenschappen gecombineerd met voorbeelden van toepassingen door *social engineering*.

WEERBAARHEID DOOR HERKENNING

Social engineeringaanvallen nemen toe in geraffineerdheid. Er zijn diverse sites en tools beschikbaar, waaruit potentiële computerkrakers ideeën vandaan kunnen halen voor het verzamelen van informatie en bijvoorbeeld voor het effectief opstellen van mail waaraan malware is gekoppeld. Voorafgaand aan het versturen, kunnen deze e-mails aangeboden worden aan een speciale 'wasstraat' om te controleren of de e-mail met gevoegde malware door anti-virussoftware, firewalls en/of spamfilters wordt herkend. Programmeerkennis is geen noodzakelijke vereiste omdat er allerlei hackerapplicaties beschikbaar zijn.
Het is niet ondenkbaar dat infiltranten ook via direct contact met een medewerker van defensie in de systemen proberen te dringen. Kennis van de risico's van sociale media voor informatiebeveiliging, kan bewustere omgang hiermee bevorderen. In dit artikel zijn een aantal beïnvloedingstechnieken besproken met de verwachting dat het met deze kennis makkelijker wordt om een social engineeringaanval te herkennen en hierdoor weerbaarder te zijn tegen zulke gebeurtenissen. De privé informatiebeveiliging en persoonlijke veiligheid kan hiermee worden verbeterd, maar dit kan ook de informatiebeveiliging binnen Defensie ten goede komen.

Psychologische of sociologische eigenschap	*Voorbeelden*
Emotie prikkelt vaak de aandacht en kan nbewust) gedrag versterken.	Oproepen van emoties, zoals angst, verdriet, irritaties, blijdschap en dankbaarheid. Mensen hebben sterkere emoties als een onderliggende waarde wordt aangesproken zoals een ideologie. Informatie om hierop in te kunnen haken wordt via sociale media of het Internet gezocht. Urgentie versterkt de emotie.
Mensen vinden erkenning en beloningen fijn, vooral financiële vooruitzichten.	Financiële prikkels worden veel gebruikt omdat het effect hiervan groot is. Een voorbeeld is: 'Je hebt een geldbedrag gewonnen', waarna je op een link moet klikken voor verdere informatie.
Een mens wil zich belangrijk voelen.	Je als een winnaar te laten voelen, bijvoorbeeld 'speciaal voor jou geselecteerd' of 'je bent precies de 100 000ste'. Als mensen op een geloofwaardige manier worden gecomplimenteerd, zijn ze ook meer geneigd te praten.
Een mens wil iets dat anderen niet hebben.	Creëer een gevoel van schaarsheid, bijvoorbeeld door de termen te gebruiken 'beperkte oplage', 'tijdelijk beschikbaar'. Dit kan verder worden versterkt door het interessegebied van het doelwit
Mensen zijn vaak inherent gehoorzaam, vooral aan autoriteiten.	Door spoofing technieken, kan het soms lijken of de mail van een bekende komt, bijvoorbeeld een hogere functionaris uit de organisatie, met het verzoek om een document in te zien. Mensen hebben de neiging om dan te gehoorzamen. Experimenten zoals die van Milgram en recente soortgelijke onderzoeken, illustreren dat.
Mensen willen graag beleefd zijn.	Als iemand een vraag stelt, ervaren mensen de neiging om te antwoorden. De vraag kan direct, maar ook indirect worden gesteld.
Mensen vinden het prettig om anderen te helpen.	E-mails met verdrietige verhalen, waarbij hulp of ondersteuning wordt gevraagd. Via een gepaste context wordt deze benadering ook via de telefoon of via face to face contact gebruikt.
Mensen willen positief en consistent zijn.	'U wilt toch ook…' Mensen worden met kleine stapjes geleid om steeds ja te laten zeggen, het wordt dan lastiger om 'nee' te zeggen.
Principe van wederkerigheid.	Als iemand iets ontvangt of een ander maakt een toegeving, creëert dit gevoelsmatig een type wanbalans in de relatie. De bevoordeelde heeft de wens om iets terug te willen geven. Vervolgens komt er een verzoek (bijvoorbeeld het klikken op een link), en wegens een sterke wens om de wederkerigheidsbalans te herstellen, wordt aan het verzoek voldaan. Dit wordt verder versterkt als datgene wat je hebt gekregen een positieve emotie oproept omdat het je interesse heeft of overeenkomt met een ideologie waarmee je je verbonden voelt.
Mensen voelen zich meer verbonden met mensen die dezelfde belangstelling delen.	Door gepaste informatie te verzamelen uit de sociale media, kan een gedeelde interesse makkelijker worden gevonden of geacteerd.
Mensen zijn nieuwsgierig	Een usb-stick kan doelgericht worden geplaatst bij een belangrijke speler in een organisatie. De meeste mensen kunnen de verleiding niet weerstaan om de usb-stick in het systeem te plaatsen.