WHITEPAPER

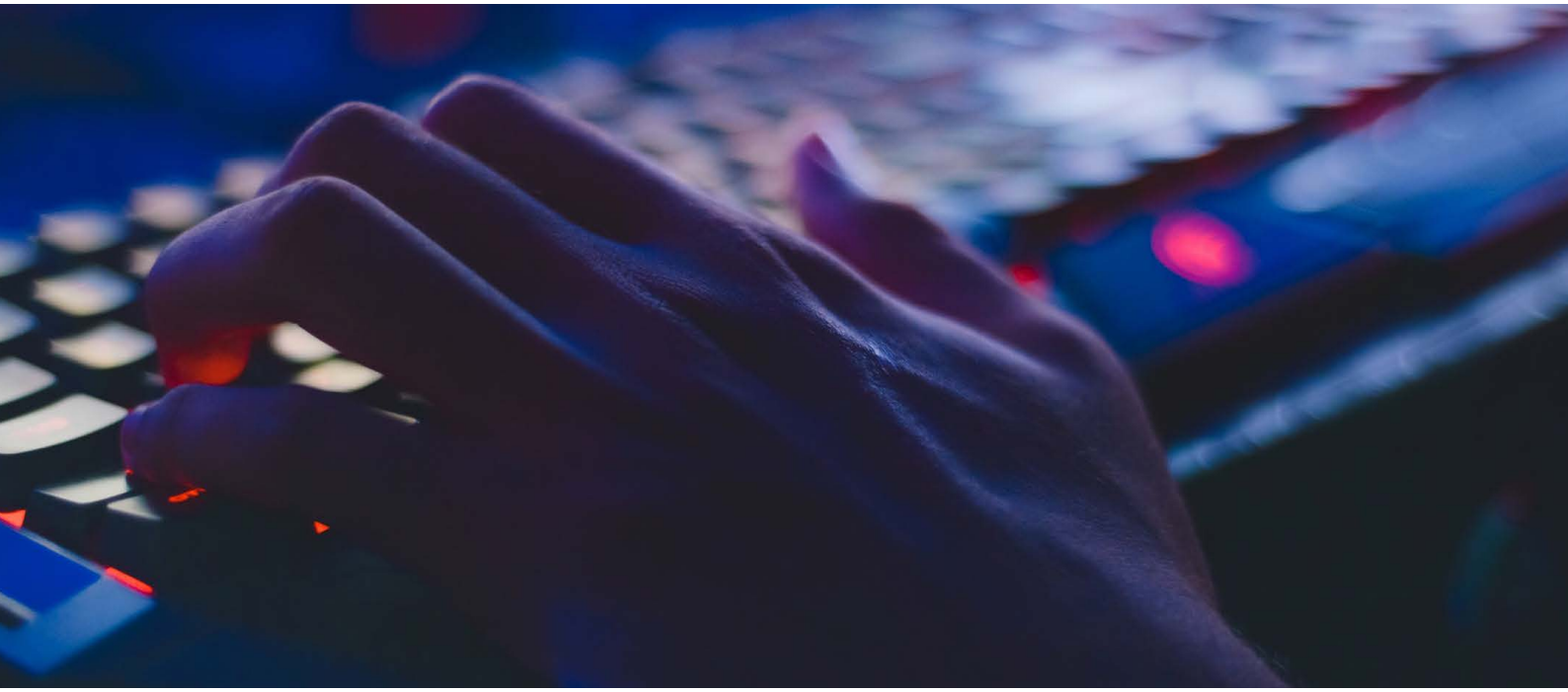
WAPEN UZELF EN UW ORGANISATIE TEGEN SOCIAL ENGINEERING

Social engineering of social hacking is een bijzondere tak van sport waartegen maar weinig mensen zijn bestand.

SECURITAS

De kunst van het misleiden

Wapen uzelf en uw organisatie tegen social engineering



Social engineering of social hacking is een bijzondere tak van sport waartegen maar weinig mensen zijn bestand. Door middel van psychologische trucs kunnen mensen zo worden gemanipuleerd dat ze dingen doen die ze niet willen doen en toegang geven tot vertrouwelijke gegevens. In deze whitepaper leest u over de methodes die worden toegepast en hoe u uzelf en uw organisatie kunt wapenen.

De kunst van het misleiden van mensen, dat is waar het bij social engineering om draait. Het is een instrument dat vaak wordt gebruikt door cybercriminelen. Bijvoorbeeld om mensen geld af te troggelen, bedrijfsgevoelige informatie te achterhalen of ter voorbereiding van een criminele of terroristische daad. Social engineering is gevaarlijk en effectief. Een van de redenen daarvoor is dat de methode gericht is op mensen in plaats van systemen.

Zwakste schakel

'Het is heel gemakkelijk om mensen in de maling te nemen', zegt Mark van den Wijngaard, veiligheidsspecialist bij Securitas. 'Dat lukt niet alleen bij medewerkers binnen een organisatie, maar ook bij directieleden en managers. Niet het systeem, maar de mens blijkt vaak de zwakste schakel. Hoewel de mens van nature misschien argwanend is, zijn we ook gevoelig voor complimenten en wederkerigheid. Social engineers maken daar misbruik van door welbespraakte mensen in te zetten die snel het vertrouwen van anderen weten te winnen.'

De kunst van het misleiden

Wapen uzelf en uw organisatie tegen social engineering

Psychologische trukendoos

Social engineers manipuleren hun slachtoffers in hun poging ze te misleiden. Een compliment geven bijvoorbeeld is een veel gebruikte tactiek. Of ze spelen in op de nieuwsgierigheid van mensen. De volgende beïnvloedingsprincipes en (psychologische) trucs worden regelmatig toegepast:

1. Opbouwen van een relatie

Criminelen proberen in het sociale circuit te komen van mensen die ze nodig hebben om informatie te krijgen over bijvoorbeeld hun bedrijf, een locatie, een proces, een systeem of goederen die ergens liggen opgeslagen. Ze komen met hun (soms kwetsbare) slachtoffer in contact via social media of een sociale gelegenheid. Hebben ze een persoon eenmaal voor zich gewonnen dan zal er altijd een moment komen dat hij zijn positie gaat gebruiken. Ofwel om informatie te krijgen dan wel om iemand iets te laten doen wat hij of zij eigenlijk niet wil doen.

2. Voordoen als autoriteit of expert

Veel mensen zijn gevoelig voor autoriteit. Criminelen weten dat ook. Op het moment dat zij zich bijvoorbeeld voordoen als rijksambtenaar of een belangrijk persoon met een hogere functie werkt dat in op de psyche van de ander. Deze zal eerder meewerken en bereid zijn (vertrouwelijke) informatie te geven. Zeker als het om een 'urgent' verzoek gaat waarbij het slachtoffer de werkzaamheden van deze persoon niet durft te belemmeren. Ook een social engineer verkleed als loodgieter of brandweerman maakt vanwege zijn expertise kans om toegang te krijgen tot een organisatie.

3. Sympathie opwekken

Mensen zeggen het liefst 'ja' tegen mensen die ze mogen. Social engineers zijn daarom vaak goede verleiders. Ze zorgen ervoor dat mensen ze aardig vinden. Hoe ze dat doen? Bijvoorbeeld door extra aandacht te besteden aan hun uiterlijk, door te vleien en interesses te veinzen. Uit onderzoek blijkt dat positieve opmerkingen altijd leiden tot sympathie, of ze nu waar zijn of niet.

4. Wederkerigheid

Wederkerigheid is een van de sterkste overtuigingprincipes die er zijn: de drang om te moeten compenseren wat andere mensen ons hebben gegeven. De bekende gedragsonderzoeker Robert Gialdini schrijft het sterke effect van deze regel toe aan het feit dat vrijwel iedereen heeft geleerd ons aan deze regel te houden: als je iets krijgt, dan doe je iets terug. Doe je dat niet dan volgen sociale sancties en vinden mensen je een profiteur, ondankbaar of een egoïst.

Informatie prijsgeven

'Mensen zijn in het begin vaak nog wel alert, dat hebben ze geleerd. Maar zodra ze het gevoel hebben dat iemand te vertrouwen is, dan geven ze alles', zegt Van den Wijngaard. 'Dat gaat soms ver. Zo blijkt uit onderzoek dat mensen gemakkelijk informatie prijsgeven via e-mail en dat medewerkers van salarisadministraties zelfs bereid zijn telefonisch een Burgerservicenummer door te geven als ze denken met een medewerker te maken te hebben die het hard nodig heeft.'

Geen achterdocht

'Mensen willen graag helpen', vervolgt hij. 'Als ik opbel als arbo-arts en zeg dat ik een onderzoek doe naar de arbo-omstandigheden dan werken de meeste mensen mee. Zeker als ik ze vertel dat we het belangrijk vinden dat ze prettig hun werk kunnen doen. De eerste vragen zijn onschuldig: 'Heb je het naar je zin? Is je bureau hoog genoeg? Zit je stoel lekker?' Bij vraag zes: 'Hoeveel beveiligers hebben jullie?', zijn mensen zo vertrouwd dat ze geen achterdocht meer voelen. Vervolgens kun je zelfs hun personeelsnummer en het wachtwoord van hun computer vragen.'

On- en offline methodes

Methodes die door (cyber)criminelen worden gebruikt vinden zowel online als offline plaats.

- Social engineers vergaren gevoelige informatie via lokmails of door onder valse voorwendselen medewerkers te bellen en gebruikersnamen en wachtwoorden te ontfutselen (phishing). Daarnaast winnen ze informatie in via het internet over medewerkers van een bedrijf.
- De USB-drop is een methode waarmee (cyber)criminelen toegang proberen te krijgen tot informatie en systemen. USB-sticks worden bijvoorbeeld ergens achtergelaten, uitgedeeld of letterlijk in een tas gedropt.
- Een kwaadwillende kan ook fysiek een bedrijf binnendringen als deze door bijvoorbeeld een HR-afdeling als sollicitant wordt voorgedragen.
- Een combinatie van aanvalstechnieken is mogelijk. Zo kan een phishingmail worden aangekondigd door een beller die een aantal gerichte vragen stelt over onderwerpen waar iemand beroepsmatig of privé interesse in heeft. Ook worden ransomware en malware vaker als bijlage toegevoegd aan phishingmails. Op een link klikken is dan niet meer nodig, het openen van de bijlage is voldoende om te worden besmet.

Malware en ransomware

Malware is een verzamelnaam voor schadelijke en ongewenste software. Deze software heeft als doel: uw privacy schenden, schade aan uw computer aanbrengen of de normale werking van uw computer verstoren. Ransomware oftewel gijzelsoftware is een chantagemiddel. Letterlijk vertaald betekent ransom: losgeld. Het werkt als een soort 'gijzeling van de computer'. De computer wordt geblokkeerd en je kunt er niets meer mee. Ransomware is in feite malware waarmee criminelen proberen om je 'losgeld' te laten betalen om ervan af te komen. Betalen blijkt echter niet (altijd) tot ontsluiting van de besmet geraakte computer te leiden, zo waarschuwt de Nederlandse overheid. Zelfs wanneer na betaling de code succesvol wordt gebruikt, blijft de software op de computer staan en kan deze enkele maanden later opnieuw het systeem blokkeren en om nog meer geld vragen.

Tijdsdruk

Tijdens een social engineering aanval moet een slachtoffer vaak snel anticiperen. Zo wordt in phishingmails regelmatig gedreigd met het blokkeren van bankpassen en accounts wanneer de ontvanger niet binnen 24 uur reageert. Het slachtoffer heeft dan geen tijd om onderzoek te doen en maakt zijn of haar keuze op basis van de beperkte informatie die op dat moment (door de social engineer) wordt aangereikt.

Informatie is het nieuwe goud

'Cybercrime, identiteitsfraude en bedrijfsspionage vormen de top drie van huidige dreigingen', zegt Van den Wijngaard. 'Informatie is het nieuwe goud en daarvan komt steeds meer beschikbaar. Tegelijkertijd is bedrijfsspionage gemakkelijker geworden. Voor kwaadwillenden is het vaak slechts een kwestie tijd om alle puzzelstukjes te verzamelen en een compleet beeld te verkrijgen.'

Wapen (en train) uzelf

Social engineering kan volgens Van den Wijngaard alleen maar worden tegengegaan door de bewustwording te vergroten. Bijvoorbeeld door middel van training: klassikaal of door middel van e-learning. Het uitvoeren van scenario's op locatie (Red Teaming) is een goede manier om mensen daadwerkelijk te laten ervaren hoe social engineering in de praktijk gaat.

'Bij Red Teaming testen we real live de awareness in een organisatie door met behulp van social engineering informatie bij een bedrijf weg te nemen. Het doel is medewerkers te laten leren, de awareness te vergroten en een lerende organisatie te ontwikkelen.'

Dit soort programma's blijken effectief. Van den Wijngaard: 'Awareness-programma's maken mensen bewust. Ze leren mensen dat je bij normafwijkingen nooit privacygevoelige informatie moet prijsgeven. Als je gebeld wordt door de ING bijvoorbeeld, dan moet er een alarmbelletje afgaan. Is een aanbieding te mooi om waar te zijn? Dan klopt het vaak niet.'

Kijken: Social Engineering Starbucks

Wat doe je als het hoofdkantoor belt en je verzoekt geen informatie te geven als het hoofdkantoor belt?

Veilig online: wees cybercriminelen te slim af:

- Wees voorzichtig met onbetrouwbare koppelingen naar nepsites of pagina's met (nep)nieuws. Bij groot nieuws zetten cybercriminelen valstrikken uit met koppelingen naar video's of foto's die moeilijk zijn te weerstaan. Wees ook voorzichtig met nieuws over beroemdheden. Voordat u het weet is uw computer besmet met malware.

- Reageer niet op verdachte e-mails met urgente meldingen over de veiligheid van uw systemen of financiën waarop onmiddellijk actie moet worden ondernomen zoals het openen van een bijlage of het doen van een online betaling.

- Lijkt een aanbieding te mooi om waar te zijn? Dan is dat vaak zo. In de meeste gevallen leiden koppelingen niet naar een fantastische aanbieding, maar naar een site met malware.

Beveilig uw informatie

Naast awareness-programma's is het belangrijk om goed na te denken over de waarde van informatie binnen een bedrijf. 'Informatiebeveiliging wordt steeds belangrijker. Je moet dus goed weten wie je toegang geeft tot welke informatie. Kwalificeer informatie en stel vast tot welk niveau medewerkers toegang krijgen tot bepaalde informatie. De centrale vraag daarbij is steeds: 'Is er sprake van need to know, of nice to know?'

'Een ander belangrijk thema is een zorgvuldige screening van mensen. Zeker op vertrouwensposities', zegt Van den Wijngaard. Er wordt volgens hem vaak slecht gescreend, referenties worden nauwelijks gecheckt. Aandacht voor het proces is daarom belangrijk. 'Het veiligheidsbewustzijn binnen een organisatie is pas effectief wanneer dit wordt gewaarborgd in een continu proces. Dat betekent dat organisaties het risico van bedrijfsspionage en van cybercrime moeten opnemen in hun risicoprofiel. Zij moeten accepteren dat het gebeurt om het vervolgens in securityplannen te kunnen vertalen in concrete maatregelen.'

De oplossing?

Dat het veiligheidsbewustzijn omhoog moet staat vast. Gemakkelijk is dat echter niet, waarschuwt Van den Wijngaard. 'Eigenlijk zou er een waarschuwingslampje moeten gaan branden zodra iemand te maken krijgt met social engineering. Het lastige alleen is dat alles wat we denken, doen en uitvoeren is gebaseerd op onze eigen ervaringen. Zolang mensen zelf nog geen slachtoffer zijn geworden van social engineering is het moeilijk om dit bewustzijn tussen de oren te krijgen. Mensen vormen daardoor de sterkste, maar tegelijkertijd de zwakste schakel.'

Must read: De kunst van het misleiden

Een boek dat elke beveiligingsprofessional gelezen moet hebben is het boek The art of intrusion oftewel: 'De kunst van het misleiden' van Kevin Mitnick. De legendarische hacker onthult hoe je je beschermt tegen het grootste veiligheidsrisico dat er is: de mens. Aan de hand van realistische scenario's geeft hij inzicht in de menselijke aspecten van informatiebeveiliging en geeft hij een kijkje in de complexe geest van een hacker.

Bedankt voor het lezen van deze whitepaper. Heeft u nog vragen over het onderwerp? Neem dan gerust contact met ons op via info@securitas.nl of 088 322 11 00.

Een nieuwe kijk op beveiliging

De missie van Securitas is om deze continu veranderende wereld te transformeren naar een veiligere plek om in te leven en werken. Securitas staat voor een proactieve, integrale en gastvrije aanpak met een digitaal hart. Deze nieuwe kijk op beveiligen resulteert in preventieve oplossingen met maximale synergie tussen mens, kennis en technologie. Securitas is dé innovatieve partner voor beveiligingsoplossingen. Nu en in de toekomst.

SECURITAS