De wetenschap van corrupt gedrag van mensen op het internet.

Attention Control?

Social engineering gaat om het bewust manipuleren van sociaal gedrag met als doel vertrouwelijke gegevens of geld te krijgen van het slachtoffer.

Daarbij gebruiken cybercriminelen oplichtingstechnieken die misbruik maken van menselijke eigenschappen

en de manipulaties door middel van technologie.

Als Anti social engineer houd je je bezig met technische ontwikkelingen op het gebied van IT, bouw, infra, mechaniek of landbouw.

Een Anti social engineer heeft veel betekenis voor veranderingen op de veiligheid van de samenleving.

Een Anti Social Engineer werkt aan technische oplossingen op wetenschappelijk, wiskundig, economisch, technisch, sociaal of praktisch gebied.

Social engineering is de term die wordt gebruikt voor een breed scala aan kwaadaardige activiteiten die worden uitgevoerd door menselijke interacties . Het maakt gebruik van psychologische manipulatie om gebruikers te misleiden tot het maken van beveiligingsfouten of het weggeven van gevoelige informatie. Social engineering-aanvallen vinden plaats in een of meer stappen.

Kennis is impact.
Weten wat werkt en wat niet.

Het inzetten van intelligentie
Kennis en macht?
Wat we al weten
Wat we nog niet weten
Wat we willen weten
Wat we niet willen weten
Wat we niet kunnen weten
Wat we wel kunnen weten

Weten met wie je te doen hebt
Weten wie wie is
Weten wat diegene doet
Weten wat diegene wil doen

Weten wat diegene niet wil

Wat mensen willen leren
Lichaamshouding
Ademhalingsrust
Stress los laten
Angst overwinnen

Phishing, vishing en smishing zijn veelvoorkomende vormen van social engineering-aanvallen, waarbij de laatste twee subvarianten zijn van de eerste. Bij alle drie wordt er een vertrouwd merk of figuur geïmiteerd om het slachtoffer ertoe te verleiden persoonlijke informatie te verstrekken.

Phishing. Phishing is een vorm van internetfraude waarbij criminelen proberen persoonlijke of bedrijfsmatige gegevens te stelen via e-mailberichten. ...
Telefoonfraude (vishing) ...
Sms-phishing (smishing) ...
WhatsApp-fraude (vriend in nood-fraude)

Het inzetten van emoties
Influencing people
Communicatief
Ideeën en het zelfbeeld
Verhalen, gedachten, gevoel
Inspelen op empathie

Behavior complementation
Beinvloeden door gedrag

Iemand leider maken
door zelf onderdanig te zijn

Social Engineering
Social engineering is een methode die criminelen gebruiken om een ander te overtuigen gevoelige informatie te delen.
Dit doet die persoon door in te spelen op menselijke (of sociale) eigenschappen, zoals nieuwsgierigheid, behulpzaamheid en vertrouwen, maar ook onzekerheid, angst of gierigheid.

Social engineering is een manipulatietechniek die gebruik maakt van menselijke fouten om private en waardevolle informatie of toegang te verkrijgen

Spam is op zich geen social engineering, maar sommige campagnes maken gebruik van social engineering-technieken zoals phishing, spearphishing, vishing, smishing of het verspreiden van schadelijke bijlagen of links.

Phishing is het meest voorkomende type social engineering-aanval, waarbij doorgaans gebruik wordt gemaakt van vervalste e-mailadressen en links om mensen ertoe te verleiden inloggegevens, creditcardnummers of andere persoonlijke informatie te verstrekken.

Hoewel phishing een voorbeeld is van social engineering, vallen niet alle social engineering-aanvallen onder phishing. Het doel van phishing is om het slachtoffer op een link te laten klikken die malware op hun apparaat kan downloaden, hun gevoelige gegevens kan stelen of hun kan omleiden naar een gespoofte website.

Waarom mensen mensen helpen en waarom niet

Social engineering is de term die wordt gebruikt voor een breed scala aan kwaadaardige activiteiten die worden uitgevoerd door menselijke interacties . Het maakt gebruik van psychologische manipulatie om gebruikers te misleiden tot het maken van beveiligingsfouten of het weggeven van gevoelige informatie. Social engineering-aanvallen vinden plaats in een of meer stappen.

Er zijn verschillende soorten social engineering-aanvallen, die allemaal frauduleuze praktijken gebruiken om het slachtoffer ertoe te verleiden privé-informatie te verstrekken. Deze tactieken omvatten baiting, scareware, pretexting, phishing, spear phishing, smishing, water holing, quid pro quo, honey trap, tailgating, rogue en vishing .

Vishing (een combinatie van de woorden 'voice' en 'phishing') is een vorm van oplichting via de telefoon waarbij de oplichters proberen om het slachtoffer te misleiden om persoonlijke, financiële of veiligheidsinformatie te geven of om geld aan hen over te maken.

Emotionele manipulatie

Cybersecurity Awareness: Social Engineering
Doelgroep
Iedereen die zich verder wil verdiepen in dit onderwerp en zich eventueel wil voorbereiden op de toekomst.

Mee helpen zoeken naar oplossingen en verbeteringen

U zet uw eerste stappen in de wereld van social engineering en wil graag meer kennis opdoen

U wilt inzicht krijgen in de gevaren van social engineering, de werkwijze van een social engineer en de preventiemaatregelen

U wilt de weerbaarheid van uw organisatie tegen social engineering kunnen vaststellen

An Anti Social Engineer reveals the secret methods hackers and con artists use to manipulate their targets and scam their victims

Houd software en firmware regelmatig up-to-date, met name beveiligingspatches . Gebruik uw telefoon niet geroot, of uw netwerk of pc in de beheerdersmodus. Zelfs als een social engineering-aanval uw gebruikerswachtwoord voor uw 'gebruikers'-account krijgt, kunnen ze uw systeem niet opnieuw configureren of er software op installeren.

Wat is baiting? Het Engelse werkwoord 'to bait' betekent 'van lokaas voorzien'. Baiting wordt, net als andere vormen van social engineering zoals mail-phishing en voice-phishing, door cybercriminelen gebruikt om toegang te krijgen tot uw netwerk, financiële gegevens en/of bedrijfsgeheimen.

Een voorbeeld van oplichting.
Via een link wordt u naar een website van oplichters gestuurd, waar ze uw betaalgegevens binnen weten te hengelen: daarom heet deze manier van bankfraude phishing. De phishing-mails zien er bedrieglijk echt uit, met logo's en zelfs een handtekening van uw contactpersoon of de directeur.

98% van de cyberaanvallen is gebaseerd op social engineering. Een gemiddelde bedrijfsorganisatie krijgt jaarlijks te maken met meer dan 700 social engineering-aanvallen. 90% van de datalekken richt zich op het menselijke element om toegang te krijgen tot gevoelige bedrijfsinformatie.

Wanneer malwareontwikkelaars social-engineeringtechnieken gebruiken, kunnen ze een onoplettende gebruiker ertoe verleiden een geïnfecteerd bestand te openen of op een koppeling te klikken die naar een geïnfecteerde website leidt. Veel e-mailwormen en andere typen malware maken gebruik van deze methoden.

Wormaanvallen
De cybercrimineel probeert de aandacht van de gebruiker te vestigen op de koppeling of het geïnfecteerde bestand en de gebruiker ertoe te verleiden hierop te klikken.

Mijn account

Social Engineering

Wanneer malwareontwikkelaars social-engineeringtechnieken gebruiken, kunnen ze een onoplettende gebruiker ertoe verleiden een geïnfecteerd bestand te openen of op een koppeling te klikken die naar een geïnfecteerde website leidt. Veel e-mailwormen en andere typen malware maken gebruik van deze methoden.

Wormaanvallen
De cybercrimineel probeert de aandacht van de gebruiker te vestigen op de koppeling of het geïnfecteerde bestand en de gebruiker ertoe te verleiden hierop te klikken.

Voorbeelden van dit type aanval:

De worm LoveLetter, die er in het jaar 2000 voor zorgde dat veel mailservers van bedrijven overbelast raakten. Slachtoffers ontvingen een e-mail waarin ze werd gevraagd de bijgevoegde liefdesbrief te openen. Als ze het bijgevoegde bestand openden, kopieerde de worm zichzelf naar alle contactpersonen in het adresboek van het slachtoffer. Deze worm wordt nog altijd beschouwd als een van de meest vernietigende aller tijden vanwege de enorme financiële schade die de worm aanrichtte.
De e-mailworm Mydoom die in januari 2004 opdook, maakte gebruik van technische berichten die afkomstig leken te zijn van de mailserver.
De worm Swen bestond uit een bericht dat afkomstig leek te zijn van Microsoft. In dit bericht stond dat de bijlage een patch was waarmee beveiligingslekken in Windows konden worden opgelost. Het was dan ook niet vreemd dat veel mensen deze boodschap serieus namen en de nep-patch installeerden, die in werkelijkheid een worm was.
Verspreidingskanalen voor koppelingen naar malware
Koppelingen naar geïnfecteerde sites kunnen worden verzonden via e-mail, ICQ en andere chatsystemen, of zelfs via IRC-internetchatrooms. Mobiele virussen worden vaak verspreid via sms-berichten.

Welke verspreidingsmethode er ook wordt gebruikt, meestal bevat het bericht in het oog springende of intrigerende woorden waarmee de nietsvermoedende gebruiker wordt verleid op de koppeling te klikken. Met deze methode voor het binnendringen van een systeem kan de malware de anti-virusfilters van de mailserver omzeilen.

P2P-netwerkaanvallen (Peer-to-Peer)
P2P-netwerken worden ook gebruikt om malware te verspreiden. Een worm of trojan verschijnt in het P2P-netwerk en krijgt een naam die de aandacht trekt, zodat gebruikers worden verleid om het bestand te downloaden en te openen. Voorbeelden:

AIM & AOL Password Hacker.exe
Microsoft CD Key Generator.exe
PornStar3D.exe
Play Station emulator crack.exe

Voorkomen dat slachtoffers melding maken van de malware-infectie
In sommige gevallen nemen de ontwikkelaars en distributeurs van malware stappen die de kans verkleinen dat slachtoffers een infectie melden:

Dit is bijvoorbeeld het geval wanneer slachtoffers reageren op een nepaanbieding voor een gratis hulpprogramma of een handleiding waarbij het volgende wordt beloofd:

Gratis toegang tot internet of mobiele communicatie
De kans om een programma voor het genereren van creditcardnummers te downloaden
Een methode om het rekeningsaldo van het slachtoffer te verhogen, of andere illegale voordelen
In dergelijke gevallen zal het slachtoffer niet snel geneigd zijn om zijn of haar eigen illegale bedoelingen te onthullen wanneer de download een trojan blijkt te zijn. Daarom is de kans klein dat het slachtoffer de infectie meldt bij een wethandhavingsdienst.

Een ander voorbeeld van deze techniek is de trojan die werd verzonden naar e-mailadressen die waren gestolen van een wervingswebsite. Mensen die zich op de site hadden geregistreerd, ontvingen nepwerkaanbiedingen die een trojan bevatten. De aanval was hoofdzakelijk gericht op zakelijke e-mailadressen, omdat de cybercriminelen wisten dat het personeel dat de trojan ontving de werkgever niet zou willen vertellen dat hun computer geïnfecteerd was geraakt terwijl ze op zoek waren naar een andere baan.

Ongebruikelijke social-engineeringmethoden
In sommige gevallen gebruiken cybercriminelen complexe methoden om een cyberaanval uit te voeren. Bijvoorbeeld:

De klanten van een bank ontvingen een nepmail die van de bank afkomstig leek te zijn en waarin hun werd gevraagd hun toegangscodes te bevestigen. Dit gebeurde echter niet via de gebruikelijke e-mail- of internetroutes. In plaats hiervan werd de klant gevraagd het formulier in de e-mail af te drukken, zijn of haar gegevens in te vullen en het formulier te faxen naar het telefoonnummer van de cybercrimineel.
In Japan gebruikten cybercriminelen een thuisbezorgingsservice om cd's te verspreiden die waren geïnfecteerd met trojanspyware. De schijven werden afgeleverd bij de cliënten van een Japanse bank. De adressen van de cliënten waren eerder al gestolen uit de database van de bank.

Een onderzoek naar online veiligheid en de mogelijkheden te vergroten om corruptie tegen te gaan.

Gemaakt door Stijn Gabeler
van Stichting GoDoGood
Voor de podcast NotebookLM