DOOR LUCINDA STERK

Social engineering: het hacken van mensen

Je hebt hackers die systemen hacken, en je hebt hackers die mensen hacken. Die laatste categorie noemen we social engineers. Ze maken gebruik van psychologie en mensenkennis om toegang te krijgen tot belangrijke data, servers, gebouwen en wachtwoorden. Social engineers begeven zich dus, anders dan technische hackers, fysiek onder hun doelwit. Dat maakt ze tegelijk kwetsbaar én effectief.

Z-CERT's security medewerker Rik Sentveld heeft zichzelf gespecialiseerd in social engineering. Hij deed in eerdere functies ook mee aan beveiligingsoefeningen bij organisaties waarin hij met behulp van social engineering toegang probeerde te krijgen tot data. Samen met Rik verkennen we deze vorm van (digitale) dreiging. Hoe gaat een social engineer te werk? Hoe herken je het? En kan je het zelf ook gebruiken om je systemen te testen?

Wat kenmerkt social engineering ten opzichte van andere vormen van hacken?

Rik Sentveld: "De naam zegt het al. Het is sociaal. Je begeeft je als hacker onder de mensen. In tegenstelling tot de technische hacker die zich voornamelijk schuilhoudt achter een laptop. Social hackers hebben lef nodig om zich toegang te verschaffen tot hun doelwit. Ze spelen als het ware een rol. Je wilt mensen doen laten geloven dat je aanwezigheid legitiem is en wat je doet of vraagt volstrekt normaal."

Hoe doe je dat? Andere mensen iets laten geloven?

Sentveld: "Je moet heel zelfverzekerd overkomen. Sommige mensen hebben dat van nature, anderen zullen het moeten hebben van hun acteerkunsten. Wie zelfverzekerd door een organisatie beweegt, legt geen verdenking op zichzelf. Ga je zoeken en twijfelen, maakt dat je meer verdacht. Beweeg dus natuurlijk door een organisatie. Alsof je precies weet waar je moet zijn. Waar de toiletten zijn en wie waar zit. Maak jezelf minder verdacht door actief op mensen af te stappen om bijvoorbeeld een niet-machine te lenen of iets dergelijk."

Wat zijn naast zelfverzekerd overkomen, nog meer trucjes van social engineers?

"Ze maken gebruik van de klantgerichtheid en natuurlijke vriendelijkheid van mensen. Ze misbruiken het feit dat veel mensen de deur voor elkaar openhouden, ook bij deuren die alleen met een toegangspas of code te openen zijn. De social engineer draagt bijvoorbeeld veel tassen of dozen bij zich, zodat hij zijn handen vol heeft en zijn (niet bestaande of nep pasje) niet kan scannen. Soms komen social engineers binnen met een ladder of open laptop alsof ze onderhoud komen plegen aan het gebouw of het netwerk."

> "SOCIAL ENGINEERING IS GEEN DOEL OP ZICH"

Maar dit kan toch niet zo maar? We hebben toch ID-protocollen?

"Een social engineer weet die makkelijk te omzeilen. De hacker kan online al het nodige voorwerk hebben gedaan, Misschien heeft hij al contact gelegd met iemand achter de balie, die hem helpt. Misschien gebruikt hij een fake ID. Misschien praat hij zichzelf eruit. Er zijn legio manieren waarop je de gebruikelijke protocollen kan omzeilen."

Waarin schuilt het gevaar voor de zorgsector?

"De collega's uit de zorg zijn van nature heel behulpzaam en vriendelijk. Ze zullen niet snel argwanend zijn naar iemand die hun hulp vraagt. Een deur openmaken voor iemand die z'n handen vol heeft? Natuurlijk! Een werkplek zoeken voor een 'collega' van een andere afdeling? Natuurlijk! Het is absoluut niet mijn bedoeling om de zorgmedewerkers argwanend te maken. Dat zou tegenstrijdig zijn. Maar het is wel goed om de veiligheidsprotocollen te blijven opvolgen ook als er druk op je wordt gezet."

Doen social engineers dat? Druk zetten?

"ja, dat is een bekende methode. Dat doen ze bijvoorbeeld aan de telefoon door net te doen alsof ze gehaast zijn of een onrustige omgeving te creëren. Er is online en mooi filmpje te vinden van een vrouw die gegevens ontfutseld van een medewerker van de telefoonmaatschappij. Ze doet zich voor als gestreste moeder, met een bandje op de achtergrond met babygehuil. Ze acteert zo overtuigend dat ze na afloop van het gesprek belangrijke gegevens heeft gekregen van een willekeurig persoon. Dat kan in de zorg ook voorkomen. Bijvoorbeeld met financiële fraude. Een hacker doet zich voor als een leverancier of een collega van een andere afdeling. En vraagt om zo snel mogelijk een (fake) factuur over te maken. Maar dit kan net zo goed met een patiënten of cliëntendossier."

"Een ander voorbeeld is het telefonisch wijzigen van persoonsgegevens. Ondanks controlevragen is het nooit met zekerheid vast te stellen of je ook echt de juiste persoon aan de telefoon hebt. Het telefonisch wijzigen van adresdata of andere persoonsinformatie is dan ook niet aan te raden. Toch gebeurt het nog wel dat klantenservicemedewerkers onder druk van (familie van) een boze patiënt afwijken van de procedures."

Hoe herken ik een social engineer?

"Die vraag kan ik niet beantwoorden. Er is geen stereotype social engineer. Het kan iedereen zijn. En dat maakt het zo lastig om er echt iets tegen te doen. Wel kan ik adviseren om wanneer een persoon of een verzoek jou een ongemakkelijk gevoel geeft, je niet moet ingaan op het verzoek van deze persoon. Twijfel je? Raadpleeg een collega of leidinggevende. En onthoud: 'Nee' is ook een antwoord!"

Hoe groot is dit probleem werkelijk?

"Social engineering is geen doel op zich, het is een methode om informatie of data te verkrijgen. Hackers doen dat meestal via de computer, maar soms heb je special informatie nodig: een wachtwoord, een dossier, noem maar op, dat je alleen kan verkrijgen door jezelf toegang te verschaffen tot een gebouw."

Wat kan een organisatie doen aan social engineering?

"Je kan deze manier van hacken meenemen in een cyber awareness-programma. Laat mensen, met name medewerkers die veel klantcontact hebben, oefenen met ' nee' zeggen en het vasthouden aan protocollen ook onder stressvolle situaties. Leer hen om bij twijfel altijd een collega of leidinggevende te raadplegen. Normaliseer dit binnen het bedrijf. Durf te vragen naar de reden van het bezoek, zeker bij onverwacht bezoek dat niet was aangemeld. Maar het belangrijkste is om medewerkers de waarde van informatie te leren. Leer ze wat een kwaadwillende kan doen met een wachtwoord, een gebruikersnaam of een kopie van een ID-kaart. Bewustwording is de eerste stap." ■

Literatuur

Influence – Robert B. Cialdini;
Flipnosis – Kevin Dutton;
Emotions Revealed – Paul Ekman;
How To Win Friends & Influence People – Dale Carnegie

Youtube-video's over social engineering:

1.
2.

Rik Sentveld werkt als Senior Cybersecurity Support Specialist bij Z-CERT. Hiervoor was hij 24 jaar werkzaam bij het Ministerie van Defensie onder andere als netwerk- en incidentmanager en de laatste 5 jaar als cybersecurityspecialist en docent bij het Cyber Warfare & Training Centre. Zijn opgedane kennis van social engineering, OSINT en gedragsanalyse gebruikt hij tegenwoordig om de zorgsector te beveiligen.

Z-CERT
COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Z-CERT is hét expertisecentrum op het gebied van cybersecurity in de zorg en speelt een belangrijke rol in het cyberweerbaar maken van de zorgsector. Z-CERT heeft specifieke kennis van medische technologie en vormt met haar deelnemers een netwerk om gezamenlijk digitale dreigingen als ransomware, phishing, datalekken of hacken aan te pakken. Het netwerk bestaat behalve de deelnemers uit brancheorganisaties, leveranciers, andere CERTs, internationale contacten en (hackers)communities. Z-CERT verzameling informatie die nodig is om risico's of dreigingen snel te signaleren en dreigingen af te slaan.