STUDENTEN TREDEN IN VOETSPOREN CYBERCRIMINEEL OM MEER INZICHT TE KRIJGEN IN SOCIAL ENGINEERING

Social engineering is een techniek die veel gebruikt wordt door cybercriminelen. Door het slinks toepassen van beïnvloedingstechnieken op medewerkers kunnen die verleid worden om gevoelige informatie prijs te geven. In dit artikel beschrijven we de resultaten van 98 social engineeringsaanvallen op organisaties, verricht door studenten van de Haagse Hogeschool. Dit geeft meer inzicht in de kwetsbaarheden, wat kan helpen meer cyberweerbaar te worden.

Cybercrime is een veel voorkomende vorm van criminaliteit. Hacken komt bijvoorbeeld vaker voor dan fietsendiefstal (respectievelijk 4,9 en 4 procent (1)). Het gedrag van mensen wordt steeds vaker erkend als belangrijke risicofactor bij cybersecurity (2). Een schatting van Ernst en Young (3) is dat 83 procent van alle cyberincidenten te wijten is aan menselijk handelen. Cybercriminelen richten zich in hun aanvallen dan ook vaak op 'de mens'. Met behulp van allerlei verleidingstechnieken proberen ze medewerkers aan te zetten tot het uitvoeren van onveilige handelingen, zoals het invullen van gegevens op een phishingwebsite of het klikken op een link met een malwarebesmetting tot gevolg. Deze misleiding wordt ook wel social engineering genoemd. Door de medewerker te misleiden kunnen technische en fysieke beschermingsmaatregelen worden omzeild (4) (5).

Maatregelen

Organisaties – de kleinere organisaties vaker dan de grotere – hebben te weinig kennis en mogelijkheden om zich te wapenen tegen dergelijke aanvallen. Enkele technische basismaatregelen (zoals up-to-date software en een virusscanner) nemen ze vaak nog wel, maar maatregelen die medewerkers bewust moeten maken van cybergevaren, trainingen of scenario's 'Wat te doen bij een cyberaanval?' ontbreken (6). Het ontbreekt bij organisaties dus vaak aan middelen om social engineering tegen te gaan. Kennis over social engineering kan een belangrijke eerste stap zijn in het treffen van effectieve maatregelen. Belangrijke vragen hierbij zijn: Hoe gaan social engineers te werk? Hoe kunnen we social engineering ondermijnen? Welke kenmerken maken een organisatie of medewerker beïnvloedbaar?

Om organisaties te helpen aan inzicht in de eigen beveiliging en om kennis op te bouwen over social engineering voeren studenten HBO Informatie Communicatie Technologie (ICT) van de Haagse Hogeschool (HHS) jaarlijks social engineeringsaanvallen uit op organisaties. Studenten gaan in de schoenen van de cybercrimineel staan en proberen, door het beïnvloeden van medewerkers, toegang te verkrijgen tot gevoelige informatie. Zowel online, telefonisch als fysiek. Hierdoor leren studenten hoe social engineeringsaanvallen werken en hoe je mensen kunt beïnvloeden, zodat zij als toekomstig professional beter in staat zijn om zich te wapenen tegen cyberaanvallen. Bovendien maakt het de meewerkende bedrijven bewust van de gevaren van social engineeringsaanvallen. In dit artikel beschrijven we de onderliggende psychologische mechanismen van social engineering en presenteren we de resultaten van dertig groepen die in totaal 98 aanvallen op organisaties hebben uitgevoerd tussen 2015 en 2018.

Een kwetsbaarheid is vaak het onbewuste, onveilige gedrag van de medewerkers. Dit is meteen wel een lastige, ogenschijnlijk ongrijpbare schakel, want er kunnen vele oorzaken zijn van cyberonveilig gedrag. In dit artikel richten we ons op een onderdeel hiervan, namelijk: het verstrekken van of (indirect) toegang verschaffen tot gevoelige gegevens aan onbevoegden.

Onbewust automatisch gedrag

Het is van belang om te weten dat mensen vuistregels gebruiken om snel een probleem op te lossen, of een beslissing te nemen in de overdaad van beschikbare informatie (7). Beslissingen worden vaak genomen op basis van één kenmerk van de situatie. Dit wordt 'selectieve perceptie' genoemd. Vuistregels zijn noodzakelijk om te kunnen functioneren en het gebruik ervan is doorgaans een onbewust proces. Volgens Kahneman (7) is het grootste gedeelte (95%) van het menselijk gedrag automatisch en irrationeel. Slechts een beperkt gedeelte van ons gedrag is dus bewust beredeneerd. De mens gedraagt zich dan ook voorspelbaar irrationeel als het aankomt op het maken van afwegingen en keuzes (8). We willen dat keuzes ons zo gemakkelijk mogelijk worden gemaakt en we kiezen bij voorkeur voor routinematige oplossingen. En dat is, rationeel gezien, lang niet altijd de meest gunstige keuze. Overigens nemen mensen doorgaans prima beslissingen op basis van deze vuistregels, maar omdat ze automatisch en irrationeel zijn, kunnen ze worden misbruikt door cybercriminelen.

Michelle Ancher is docent bij de opleiding HBO ICT (richting Information Security Management) en onderzoeker bij het lectoraat 'Cybersecurity in het mkb' van de Haagse Hogeschool. Michelle is sociaal psycholoog en richt zich op de menselijke factor van de information security. Ze is bereikbaar via m.ancher@hhs.nl

Cybercriminelen maken gebruik van verleidingstechnieken om mensen te overtuigen om bepaalde regels te omzeilen. Een voorbeeld: als een aanvaller zich voordoet als directeur (een autoriteit) en verzoekt om vertrouwelijke data, dan zijn mensen sneller geneigd om dit te doen dan wanneer een collega of onbekende dit vraagt.

Beïnvloedingsprincipes

Gedrag is dus in de regel automatisch en kan beïnvloed worden door cybercriminelen. Er bestaan verschillende beïnvloedingsmechanismen, veelal gebaseerd op fundamentele psychologische mechanismen (9) (10).

De verleidingstechnieken van Cialdini (11) worden in marketing en (ook met succes) door social engineers gebruikt (9). Cialdini (11) beschrijft zes manieren van beïnvloeding:

- wederkerigheid (de neiging iets terug te doen als iemand ons iets geeft);
- sympathie (sneller iets aannemen van iemand die we aardig vinden, die op ons lijkt);
- sociale bewijskracht (iets doen omdat anderen dat ook doen);
- autoriteit (de neiging om de expert te volgen);
- commitment & consistentie (de neiging om consistent te blijven bij wat we eerder hebben gezegd of gedaan);
- en schaarste (iets graag willen omdat het beperkt beschikbaar is).

In het principe van schaarste zie je de theorie van 'loss aversion' (12) terug. Dit is het fenomeen dat veel keuzes niet gebaseerd zijn op rationeel de beste optie zoeken, maar op de gedachte dat verlies vermijden belangrijker is dan winst behalen. Bij schaarste zijn we bang om iets mis te lopen. Deze angst zorgt ervoor dat we niet geheel rationeel meer nadenken. Een voorbeeld: de aanvaller die zich voordoet als ICT-medewerker en verzoekt om inloggegevens, omdat anders de toegang tot de werkbestanden geblokkeerd wordt.

Daarnaast blijkt een effectieve overtuigingstechniek het zogenoemde 'distraction' (9). Dit is het afleiden van een persoon door het aanwakkeren van emoties, zoals verrassing, gejaagdheid, angst of paniek. Dit principe gebruiken criminelen om ervoor te zorgen dat personen aan een verzoek voldoen, terwijl in een 'normale' situatie die persoon dat niet zou doen (10).

Ook de sociale omgeving is een belangrijke bepalende factor van gedrag (13). De cultuur in een organisatie en bijbehorende kernwaarden bepalen voor een groot deel hoe medewerkers communiceren en hoe ze omgaan met afspraken, regels, onderlinge feedback, verantwoordelijkheden en missers. De bedrijfscultuur kan afbreuk doen aan de cyberveiligheid: een leider die zelf niet volgens de veiligheidsvoorschriften werkt, of collega's die niet veel oog hebben voor veiligheid. Ook de sector, de grootte van de organisatie (hoe meer mensen des te groter de kans op fouten) en het ontwerp van de fysieke en technische omgeving (14) hebben hun weerslag op het gedrag van medewerkers (15).

Methode

Dit artikel beschrijft een verkennend onderzoek naar vatbaarheid van organisaties voor social engineeringsaanvallen. De groepen studenten waren vrij om, in samenspraak met de opdrachtgever, een concrete invulling te geven aan het opzetten van de aanvallen, het gebruik van verleidingstechnieken en het selecteren van doelobjecten.

In totaal werden 98 aanvallen uitgevoerd op dertig organisaties. De meeste organisaties deden mee via het netwerk van de HHS. Die organisaties werden benaderd door docenten en onderzoekers. Ook benaderden organisaties de HHS zelf, omdat ze via-via gehoord hadden van de mogelijkheid om deel te nemen. Er deden organisaties mee uit diverse sectoren, zoals de overheid, de zorg, de financiële sector en diverse mkb-bedrijven, zoals softwareontwikkelaars, grafische- en metaalbedrijven.

Drie typen social engineeringsaanvallen werden gebruikt: 1. fysiek, 2. telefonisch (vishing) en 3. digitaal (phishing). Studenten bepaalden met de opdrachtgever wat voor type gevoelige informatie er bemachtigd ging worden. Variërend van elektronische dossiers tot inloggegevens van medewerkers. Bij de aanval richtte de student zich op een bepaald doelobject, in feite de sleutel tot de gevoelige informatie: een medewerker (in totaal 71 keer), een locatie, zoals het hoofdkantoor en daarbinnen de serverruimte (38 keer) of een object, zoals een usb-stick (4 keer).

Bij de fysieke aanval probeerden studenten op de locatie van de organisatie toegang te verkrijgen door (a) gewoon naar binnen te lopen, al dan niet met een medewerker (het zogeheten 'tailgating'), of (b) via interactie met een medewerker door zich voor te doen als iemand anders (bijvoorbeeld als auditor of stagiair facility management). Een enkele keer werd er (c) een usb-stick neergelegd om te kijken of een medewerker deze in een pc zou plaatsen.

De telefonische aanvallen waren gericht op een bepaalde persoon of afdeling voor het verkrijgen van: (1) klant- of organisatiegegevens zoals rekening- of uitkeringsgegevens,

(2) inloggegevens van medewerkers en/of (3) contactgegevens van medewerkers.

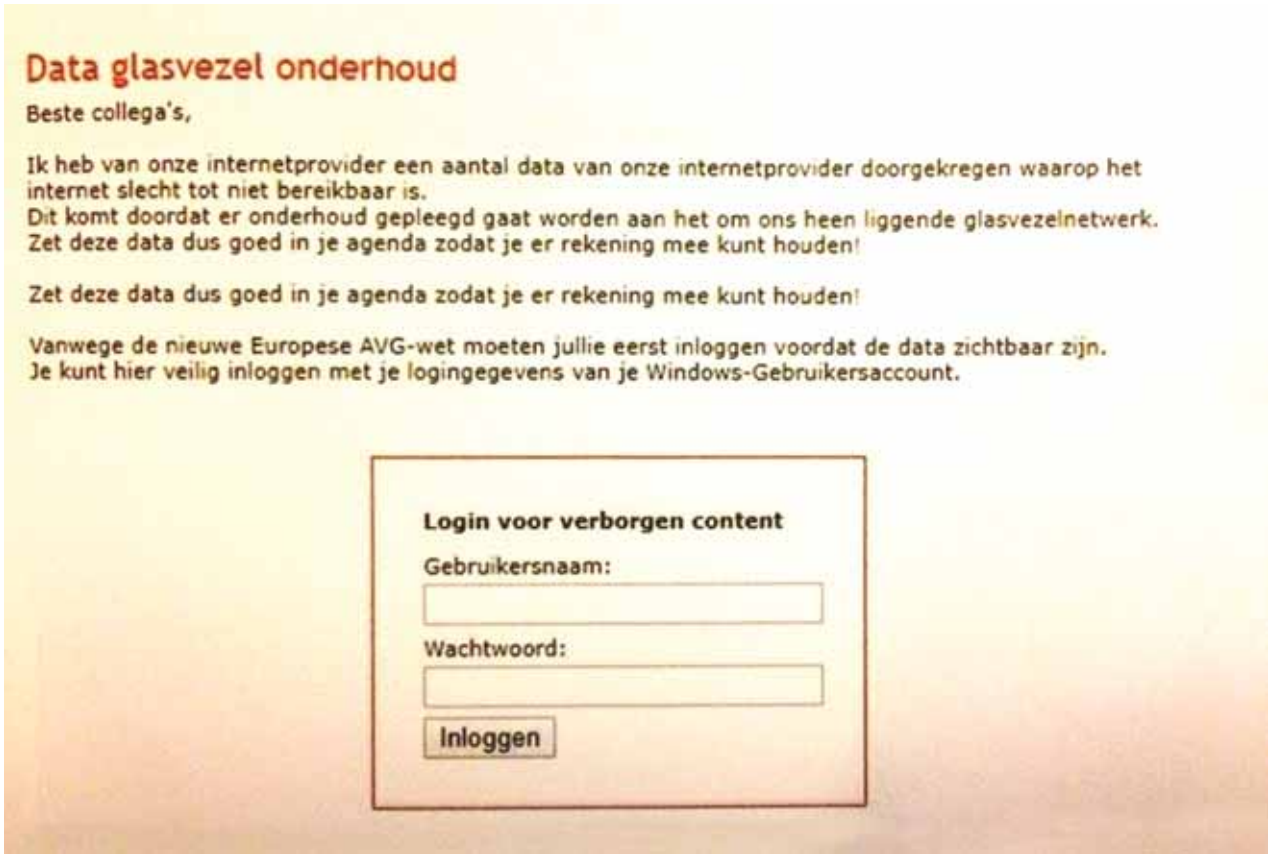
Bij de digitale social engineeringsaanvallen werden medewerkers verleid tot het aanklikken van een link in een phishingmail of tot het prijsgeven van gevoelige data via e-mail. Een voorbeeld: studenten stuurden een e-mailbericht (zogenaamd afkomstig van de directeur) met een hyperlink en het verzoek om via de hyperlink mee te doen aan een werktevredenheidsenquête. In werkelijkheid deden de medewerkers dan niet mee aan een enquête, maar werden ze omgeleid naar een phishingwebsite.

Fasen onderzoek

Studenten gingen volgens de 'social engineering attack lifecycle' (16) te werk. In de eerste fase, het vooronderzoek, brachten ze de specifieke organisatiecontext in kaart middels deskresearch, het afnemen van een cultuurscan (17) en het observeren van de (sociale) omgeving van de organisatie. Hiervoor hadden ze ongeveer 5 dagen. Vervolgens selecteerden ze een doel en één of meer overtuigingsprincipes van Cialdini (11). Het tijdstip van de aanval kon als hefboom fungeren. Bijvoorbeeld met Valentijnsdag een e-card met phishinglink versturen. Met deze input ontwierpen de studenten een aantal aanvalsscenario's (fase 2) waaruit ze de meest kansrijke kozen en de interactie aangingen met medewerkers van de organisatie (fase 3). Ze rondden de aanval af (fase 4) door de organisatie te verlaten en de opdrachtgever te informeren.

De studenten hielden zich bij de aanval aan de wet- en regelgeving. Vernieling of identiteitsfraude was bijvoorbeeld niet geoorloofd. Dat werd door de opdrachtgever en een coach van de HHS gecontroleerd. Echter, in overleg met de opdrachtgever mochten studenten wel bepaalde interne bedrijfsregels overtreden (bijvoorbeeld zichzelf toegang verschaffen tot een bedrijfsruimte) of het sturen van een phishingmail naar medewerkers. In het geval van een fysieke social engineeringaanval hadden de studenten een vrijwaringsverklaring bij zich, mochten ze ontmaskerd worden.

Om de opdrachtgever een garantie te geven dat er betrouwbaar met hun gegevens werd omgesprongen,



tekenden de studenten een geheimhoudingsverklaring. Dat betreft alle gevoelige informatie die ze zouden aantreffen bij het bedrijf. Ze stelden een protocol op voor de omgang met vertrouwelijke informatie, een ethische gedragscode en legden een Verklaring Omtrent Gedrag (VOG) voor.

Tijdens de aanval verzamelden de studenten gegevens door bijvoorbeeld het doen van observaties; het vastleggen van bewijslast op beeld of in gespreksverslagen; en door het loggen van het aantal clicks op een phishingmail. Studenten rapporteerden de geanonimiseerde resultaten aan de opdrachtgever en deden aanbevelingen voor verbeteringen. Na afloop vernietigden ze het eventueel verkregen bewijsmateriaal.

Het bleek dat bijna de helft van de aanvallen die de studenten uitvoerden succesvol was. Gelukkig voor de meewerkende organisaties lukken aanvallen lang niet altijd, maar het is opvallend dat de aanvallen van de studenten zo'n aanzienlijk succespercentage hadden.

Fysieke aanval

Van de in totaal 39 fysieke aanvallen waren er 22 succesvol (56%). Dit gebeurde door `gewoon' binnenlopen en middels tailgating (59% succesvol). Of door toegang te vragen bij de receptie door zich voor te doen als iemand anders, bijvoorbeeld als onderhoudsmedewerker van de koffieautomaat (53% succesvol). Bij drie van de vier aanvallen waar een usb-stick was achtergelaten, werd de usb-stick door de receptie of een medewerker in een pc gestoken. Bij geslaagde aanvallen werden niet gelockte computers aangetroffen en dikwijls vertrouwelijke gegevens (bijvoorbeeld een lijst met ID-gegevens). Ook lukte het in vier gevallen om toegang te krijgen tot een serverruimte. Het was de aanvallers niet gelukt om via een fysieke aanval inloggegevens te bemachtigen.
Eén derde van de aanvallers kon vrij in het gebouw rondlopen. Hierbij werden ze, op twee gevallen na, wel door een medewerker aangesproken wat ze kwamen doen. Met een smoesje kwamen de meesten hiermee weg, maar niet iedereen. Zij werden geverifieerd bij de receptie en vielen door de mand. Sympathie (de vriendelijke student die zich voordoet als zoon van een medewerkster en haar werkplek wil versieren voor haar verjaardag), autoriteit (veiligheidsinspectie of afspraak met de manager) en distraction (met een grote taart door de toegangspoort lopen) werden met succes toegepast (respectievelijk 8, 4 en 2 keer).

Een voorbeeld van een succesvolle fysieke aanval was dat studenten met een taart een toegangssysteem wisten te omzeilen. De opdrachtgever dacht dat de fysieke toegang ondoordringbaar was. De studenten deden zich voor als medewerkers van een andere locatie en liepen met de taart middels tailgating met een medewerker mee. Eenmaal binnen ging één student op onderzoek uit, terwijl de anderen met de taart voor afleiding zorgden bij het personeel door de taart te geven. Ze hadden zich van tevoren goed verdiept in de organisatiecultuur. "We kwamen erachter dat dit een trots bedrijf is dat overal zijn logo op plakt en graag successen deelt. Daarom kozen we voor een taart met daarop het logo en een felicitatie van een andere afdeling", aldus één van de studenten.

Bij de niet-succesvolle aanvallen liet de receptie de aanvaller zonder afspraak niet binnen of werden de aanvallers netjes begeleid door het pand. De medewerkers hielden zich aan het protocol en checkten in vijf gevallen de afspraak. Sympathie en autoriteit werden hier in drie gevallen zonder succes toegepast. In één geval werd de student aangesproken door een beveiligingsmedewerker: "Het viel hem op dat ik geen Apple-laptop had, terwijl iedereen daar met een Apple werkt."

Telefonische aanval

De telefonische aanvallen (33 totaal) waren minder succesvol (30% geslaagd). Telefonisch lukte het in 25% van de (8) gevallen om inloggegevens te krijgen. Dit gebeurde doordat de aanvaller zich voordeed als ICT-medewerker of als medewerker die niet kon inloggen. Hier werd het principe schaarste (tijdsdruk) gebruikt en autoriteit (ICT-medewerker met kennis van zaken). In de andere gevallen lukte het niet om inloggegevens te bemachtigen. De aanvaller werd wel geloofd, maar de medewerker hield zich aan het protocol, bijvoorbeeld door naar de identiteit van de beller te vragen. Ook de medewerkers die kennis van ICT hadden en doorvroegen, bijvoorbeeld over het zogenaamde netwerkprobleem dat er zou zijn, trapten er niet in. Twintig procent van de aanvallen op klant- of organisatiegegevens (12) slaagden met name door gebruikmaking van sympathie en wederkerigheid. Een aanvaller deed zich voor als samenwerkingspartner van de organisatie met de vraag om een relatiegeschenk te sturen naar de directeur. Ook werd distraction toegepast. De aanvaller vertelde als zogenaamd familielid dat er een misdrijf gepleegd was bij een klant (opwekken van afschuw). Bij de aanvallen waar gevraagd werd om contactgegevens (13), informatie die vervolgens gebruikt zou kunnen worden voor een gerichte aanval, slaagden er vijf en werden e-mailadressen of telefoonnummers van medewerkers gegeven. De gebruikte overtuigingsprincipes waren hier heel divers.

Een voorbeeld van een telefonische aanval is een student die zich voordeed als ICT-medewerker om inloggegevens te verkrijgen voor een elektronisch dossier. Tijdens het vooronderzoek waren gegevens van een medewerker gevonden die bevoegd was in het elektronisch dossier te werken. Ook was de naam bekend van het externe ICT-bedrijf waar de organisatie mee werkt. Er waren eerder die week al storingen geconstateerd op het netwerk, werd door de opdrachtgever verteld.
De aanval verliep als volgt: via de receptie kreeg de student in de rol van ICT-medewerker (autoriteit) de medewerker aan de lijn en legde uit dat er een dubbele loginactiviteit was gemonitord en dat een aantal andere medewerkers ook moeite hadden met inloggen (sociale bewijskracht) en gebeld waren. Voorstel was om het wachtwoord direct te wijzigen (schaarste in tijd) middels hard resetten. Het verhaal van de ICT-medewerker werd geloofd. Alleen wilde de medewerker het wachtwoord niet telefonisch doorgeven, maar stelde voor om zelf het wachtwoord te wijzigen.

Digitale aanval

Van de in totaal 26 digitale aanvallen waren er 12 succesvol (46%). Achttien aanvallen waren gericht op het laten klikken op een phishinglink, waarmee het slachtoffer malware binnen kon halen (50% succesvol). Acht aanvallen waren gericht op het verkrijgen van data van met name persoonlijke- of inloggegevens (38% succesvol).

Een succesfactor bij de digitale aanvallen is het gebruik van het principe van autoriteit (7), bijvoorbeeld doordat iemand zicht voordoet als ICT-medewerker of manager. De combinatie met sympathie blijkt volgens Ferreira nog effectiever te zijn. Dit is terug te zien bij elk van de drie aanvallen. Bij het niet-slagen was de diversiteit van gebruik van overtuigingstechnieken in de scenario's groot - wederkerigheid (2), commitment en consistentie (3) en autoriteit (7) - en is de reden lastiger te achterhalen.

Een voorbeeld van een geslaagde phishingaanval was de e-mail aan medewerkers over glasvezelnetwerkonderhoud. De mail was zogenaamd afkomstig van de directeur (principe van autoriteit) met het bericht dat ze de onderhoudsdata in hun agenda moeten zetten om problemen te voorkomen. Deze data kunnen ze zien door op een link te klikken waar ze moeten inloggen met hun account vanwege de nieuwe AVG-wet (weer autoriteit). Uit vooronderzoek kwam de opvallende schrijfstijl van de directeur, die elke zin op een nieuwe regel zet. Er is gebruik gemaakt van een domeinnaam die erg lijkt op die van de organisatie, een kopie van de website van de organisatie en een extra pagina met een loginveld.
Het resultaat was dat van de 150 e-mails er 56 zijn aangekomen. Er hebben vijftien van de 56 medewerkers op de link geklikt. Vervolgens hebben acht medewerkers hun inloggegevens ingevuld. Drie van deze medewerkers hebben dit gemeld. Voor de organisatie zijn dit acht inlogcombinaties teveel. Immers, één is al genoeg om het systeem te compromitteren.

Conclusie

Cybercrime is inmiddels een veelvoorkomende vorm van criminaliteit en organisaties hebben iedere dag te kampen met cyberaanvallen. Aanvallen richten zich daarbij vaak succesvol op de mens via social engineering. Om meer inzicht te krijgen in de vraag waarom social engineering zo goed werkt en hoe organisaties zich hiertegen kunnen wapenen, voerden studenten social engineeringsaanvallen uit op organisaties. Bijna de helft van de aanvallen was succesvol, ook bij organisaties die de basisbeveiliging dachten goed op orde te hebben. Dit geeft aan dat social engineering een serieus probleem is.

Bij succesvolle aanvallen werden verschillende beïnvloedingstechnieken gebruikt. Het principe sympathie is vaak succesvol toegepast, vooral bij een fysieke aanval. Ook is vaak, met name bij de telefonische aanval, succesvol gewerkt met de principes schaarste en autoriteit. Een andere veelgebruikte overtuigingstechniek is distraction, waarbij een emotie werd opgewekt als verrassing of afschuw. Het principe schaarste werkt ook op deze manier. Bijvoorbeeld door tijdsdruk op te leggen om inloggegevens te verstrekken, omdat anders het systeem crasht.

Het belang van vooronderzoek is duidelijk terug te zien. Het blijkt heel makkelijk om schijnbaar onschuldige informatie over medewerkers te verkrijgen via openbare bronnen, vooral social media. Deze informatie kan ingezet worden als hefboom om personeel van de organisatie te manipuleren. Door een telefoontje konden studenten eenvoudig de naam van IT-systeembeheerder achterhalen of het e-mailadres van de directeur. Een phishingmail kan dan al snel worden gemaakt. Kennis over de organisatiecontext helpt om aan te sluiten bij de herkenbare omgeving. Dit heet 'framing' en is vaak toegepast. Door observaties was bijvoorbeeld de 'dresscode' eenvoudig te achterhalen en maakte

Het demonstreren van kwetsbaarheden aan medewerkers, maakt ze bewust onbekwaam en vergroot zodoende de risicoperceptie

tailgating succesvol. Enige terughoudendheid bij het prijsgeven van schijnbaar onschuldige informatie, zoals een e-mailadres van het werk en een specifieke functie via social media, is aanbevelingswaardig.

Een bepaalde organisatiecultuur lijkt een rol te spelen in het makkelijker prijsgeven van voor cybercriminelen relevante informatie. Studenten wisten regelmatig informatie te verkrijgen over doelen door in te spelen op de servicegerichtheid van medewerkers zoals in de zorg en overheidssector. Een medewerker die zeer behulpzaam was en het leuk vond over zijn vak te vertellen, liet studenten, die zich voordeden als studenten Bouwkunde, foto's maken op een beveiligde locatie.

Sommige aanvallen waren onvoldoende voorbereid of sloten te weinig aan bij de organisatiecontext, zoals in het voorbeeld van de studenten die met een HP-laptop rondliepen in een bedrijf waar overwegend wordt gewerkt met Apple-computers. Ook bleken medewerkers met een voldoende ICT-kennisniveau minder gevoelig voor phishing te zijn.

Een belangrijke voorwaarde voor het succesvol pareren van een aanval is dat de organisatie de basisbeveiliging op orde heeft (10), zoals gedragsprotocollen, functiescheiding en toegangsbeleid. Dit geeft echter geen garantie. Studies zoals (18) (19) geven mooie aanvullende oplossingsrichtingen uit de psychologie. Hieronder bespreken we enkele van deze richtingen.

Kennis over de organisatiecultuur en bijbehorende waarden geeft input over kwetsbaarheden (18). Bovendien kan een informatieveilige cultuur gestimuleerd worden (20). De mate van sociale controle in een organisatie is belangrijk. Als deze hoog is, kan onveilig gedrag van sleutelfiguren in de organisatie, zoals het delen van wachtwoorden, snel worden overgenomen door anderen. Andersom kan dit ook werken. Als de norm het naleven van veiligheidsvoorschriften is, kan sociale controle dit gedrag versterken.

Een oplossingsrichting om te zorgen dat mensen zich bewust worden van hun automatische gedrag, is het inbouwen van vertraging in de interactie met onbekenden indien gevraagd wordt naar gevoelige informatie. Bijvoorbeeld middels een standaardprotocol om de persoon kort daarop terug te bellen, voor het checken van de identiteit (18). Of om te vragen aan onbekenden om hun verzoek te sturen via de email. Het helpt om nadrukkelijk medewerkers permissie te geven om personen te verifiëren (21). Ook technische aanpassingen zijn denkbaar om e-mails van mensen die niet voorkomen in je adresbestand, in platte tekst zonder opmaak, aan te leveren, zodat een bewuste handeling vereist is om eventuele links te openen in de browser (22).

Het ondergaan van social engineering is een interventie op zich. Het demonstreren van kwetsbaarheden aan medewerkers, maakt ze bewust onbekwaam en vergroot zodoende de risicoperceptie (23). Vooral indien mensen hier vervolgens op reflecteren (24). Ook Schaab (25) benadrukt het belang van blootstelling aan social engineering, bijvoorbeeld via rollenspelen. Hierdoor kunnen medewerkers, vooral diegenen met een sociale functie en met persoonlijkheidstrekken als volgzaamheid (18) (26), oefenen met gewenste reacties in de sociale interactie.

Ook Cialdini (11) zelf oppert oplossingsrichtingen hoe mensen en organisaties zich kunnen wapenen tegen de door hem beschreven beïnvloedingsprincipes. Neem het tegengaan van het principe sympathie. Hier kan nieuw (automatisch) gedrag worden aangeleerd. Een receptionist kan geleerd worden (in een training of game) om een mentaal script te doorlopen bij interactie met een persoon die vraagt om gevoelige informatie: 'Vind ik de persoon aardiger dan onder gegeven omstandigheden te verwachten?' en indien ja, deze relatie met de persoon loskoppelen van het verzoek dat gedaan wordt door vriendelijk te antwoorden dat het verzoek niet ter plekke ingewilligd kan worden.

Daarnaast is kennis over beïnvloeding toe te passen om medewerkers te stimuleren tot meer cyberveilig gedrag. Deze technieken kunnen toegepast worden om mensen te verleiden of aan te zetten tot meer cyberveilig gedrag. Twee voorbeelden: Speel via overtuigende communicatie in op 'loss aversion': (zonder back-up kun je al je bestanden kwijtraken). Of zet de sociale omgeving in als hefboom voor meer cyberveilig gedrag: via communicatie

met een boodschap als '80 procent van de medewerkers heeft zijn password reeds gewijzigd' kunnen medewerkers worden overtuigd om zich veiliger te gedragen. Zo maak je van de mens de sterkste schakel.

Co-auteurs

Rick van der Kleij
Rick van der Kleij is sr. onderzoeker bij het lectoraat 'Cybersecurity in het mkb' van de Haagse Hogeschool en sr. onderzoeker bij TNO. Rick is psycholoog en richt zich op cybergedrag van individuen en de cyberweerbaarheid van organisaties. Rick is bereikbaar via r.vanderkleij@hhs.nl

Rutger Leukfeldt
Rutger Leukfeldt is lector Cybersecurity in het mkb bij de Haagse Hogeschool en senior onderzoeker cybercrime en coördinator van het cybercrime cluster van het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR). Rutger is te bereiken via e.r.leukfeldt@hhs.nl

Referenties

(1) CBS. (2017). ICT kennis en economie 2017. Den Haag: Centraal Bureau voor de Statistiek.
(2) Leukfeldt. (2017). Research Agenda Human Factor in Cybercrime and Cybersecurity. Den Haag: Eleven International Publishing.
(3) EY. (2017). 10th Annual Global Information Security Survey 2017.
(4) Schneier, B. (2003). Beyond fear. Copernicus books.
(5) Mitnick. (2003). The art of deception. John Wiley & Sons Inc.
(6) Leukfeldt. (2018). De 'human' factor in cybersecurity. oratie. Den Haag: De Haagse Hogeschool.
(7) Kahneman. (2011). Thinking fast and slow. New York: Farrar, Straus and Giroux.
(8) Ariely. (2010). Predictably irrational. USA: Harper Collins.
(9) Fereirra. (2015). Principles of persuasion in social engineering and their use in phising. HAS 2015, (pp. 36-47).
(10) Gragg. (2002). A multilevel defense against social engineering. White paper, Sans Institute.
(11) Cialdini. (2017). The psychology of persuasion. HarperCollins Publishers Inc.
(12) Tversky, K. e. (1992). Advances in prospect theory: Cumulative representation of uncertainty. Journal of Risk and Uncertainty, Volume 5, Issue 4, pp 297–323.
(13) Ajzen. (1991). Theory of planned behavior. Organizational Behavior and Human Decision Processes Volume 50, Issue 2 , Pages 179-211.
(14) Johnson. (2012). Designing with the mind in mind. Morgan Kaufman.
(15) Robbins, J. (2018). Organizational behavior. UK: Pearson Education Limited .
(16) Mcafee. (2015). Hacking the Human Operating System, The Role of Social Engineering within Cybersecurity. Retrieved from http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf.
(17) Handy. (1985). Understanding Organisations , 3rd ed. Harmondsworth: Penguin.
(18) Parsons, C. (2010). Human factors in information security: individual culture en security environment. Science en technology.
(19) Fan. (2017). Social engineering: I-E based model of human weakness for attack and defense investigations. International journal of Computer Network and Information Security, 1-11.
(20) Glaspie. (2018). human factors in IS culture: a literature review 2018.
(21) Intelsecurity. (2017). Hacking the human operating system. Retrieved from http://computer weekly.com.
(22) NCCIC, N. C. (2017). Enhanced Analysis of GRIZZLY STEPPE Activity. Retrieved from http://theconversation.com/the-only-safe-email-is-text-only-email-81434
(23) Sagarin, B. J., Cialdini, R. B., Rice, W. E., & Serna, S. B. (2002). Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion.". The Journal of Personality & Social Psychology, Vol 83(3), 526-541.
(24) Hof, C. (2013). Social engineering. Soesterberg: TNO.
(25) Schaab. (2017). Social engineering defence mechanisms and counteracting training strategies. Information & Computer Security, Vol. 25 Issue: 2, 206-222.
(26) Workman. (2008). A test of interventions for security threats from social engineering. Information Management & Computer Security, Vol. 16 Issue: 5, .463-483.