SOGETI

People.
Van veilig voelen naar veilig zijn.
Hacked.

Social Engineering. Bent u veilig?

Is uw organisatie veilig?

Security staat meer dan ooit in de belangstelling. Elke dag is er wel iets over in het nieuws, in kranten, op het journaal en in de sociale media. In reactie daarop steken bedrijven veel tijd, energie en geld in allerlei technische security oplossingen, maar dat is niet altijd voldoende.

In de meeste gevallen blijkt namelijk dat de mens de zwakste schakel in het security-beleid is. De informatie waar zij beschikking over hebben, kan aantrekkelijk zijn voor een Social Engineer.

Wat is dan precies Social Engineering? Het is een vorm van 'hacken', waarbij wordt ingespeeld op de maakbaarheid van de mens. Met behulp van Social Engineering worden mensen gemanipuleerd om informatie te verschaffen of acties uit te voeren om het doel van de hacker te bereiken.

Onderzoek toont een groei van Social Engineering aan, maar in Nederland wordt er nog weinig aandacht aan deze problematiek geschonken. De kans om slachtoffer te worden van een Social Engineering aanval neemt toe en de financiële schade van een aanval kan aanzienlijk zijn.

Sogeti Social Engineering Challenge

Sogeti is continu bezig om organisaties bewuster te maken van hun kwetsbaarheid op het gebied van Security. In dat kader organiseerde Sogeti in het voorjaar van 2013 voor de 2e keer de Sogeti Social Engineering Challenge.

Waren Nederlandse organisaties in 2012 nog niet van te voren ingelicht over dit initiatief, voor de editie van 2013 meldde een aantal van hen zich zelfs spontaan aan om een aanval te 'ondergaan'.

Conclusies

De factor Mens wordt nog steeds onderschat

Werknemers zijn zich niet bewust van hun rol in informatiebeveiliging.

Belangrijke informatie is vrij toegankelijk via openbare bronnen

Bedrijven en hun medewerkers zijn zich nog onvoldoende bewust van het feit dat zij via openbare websites en social media veel bedrijfsinformatie prijsgeven.

Verschillen branches

Met name de financiële dienstverleners bleken kwetsbaar voor Social Engineering aanvallen. Een zorgelijke constatering, aangezien zij toch al vaak het doelwit van allerlei security-aanvallen zijn en de verwachting is dat dit alleen nog maar toe zal nemen.

"Gaaf!
Dit is een hele goede healthcheck voor ons en draagt bij aan onze Awareness."
ABN Amro Hypotheken Groep

De tegenaanval

Wat heeft u nodig om uw bedrijf weerbaarder te maken en de tegenaanval in te zetten?

Security Awareness

Programma's voor bewustwording, opleidingen en trainingen moeten ervoor zorgen dat mensen Social Engineering herkennen en zich bewust zijn van de impact en hun rol daarin. De programma's zijn dan zowel gericht op medewerkers in het algemeen als specifieke (kwetsbare) groepen in het bijzonder.

Fysieke beveiliging

Aanvullende maatregelen, bijvoorbeeld op het gebied van optimale fysieke beveiliging als toegangscontrole, zullen daarom ook zeker overwogen moeten worden.

Technische beveiligingsmaatregelen

Voorbeelden van technische beveiligingsmaatregelen zijn: de toepassing van sterkere authenticatie bij de toegang tot gevoelige informatie (bijvoorbeeld niet alleen een wachtwoord, maar ook een PIN-code) en het blokkeren van buitenlandse telefoongesprekken.

Beveiligingsbeleid

Het voeren van een eenduidig beveiligingsbeleid – met duidelijke do's en don'ts, gedragscodes en sancties is essentieel in het afweren van Social Engineering aanvallen.

Wat levert investeren in Security u op?

- Verlaging TCO
- Kostenbesparing incidentoplossing
- Continuïteit van core business
- Beperken gevolgschade

Ook de stap maken van veilig voelen naar veilig zijn?

- **sogeti.nl/security**
- **security@sogeti.nl**

Doet u mee aan de Sogeti Social Engineering Challenge 2014?

Inhoud

01

Voorwoord

Voorwoord

Security staat meer dan ooit in de belangstelling. Elke dag is er wel iets over in het nieuws, in kranten, op het journaal en in de sociale media. Websites worden plat gelegd met behulp van DDos aanvallen en het ene beveiligingslek is nog niet verholpen, of de volgende inbraak dient zich al weer aan. In reactie daarop steken bedrijven veel tijd, energie en geld in allerlei technische security oplossingen, maar dat is niet altijd voldoende.

In de meeste gevallen blijkt dat de mens de zwakste schakel in het security-beleid is.

Kwaadwillenden spelen hierop in en krijgen door middel van Social Engineering gevoelige bedrijfsinformatie in handen. Ze overrompelen en manipuleren nietsvermoedende medewerkers om hun doel te bereiken. Waarom zou een hacker nog moeite doen om een netwerk binnen te dringen, een applicatie te misbruiken, of een complex informatiesysteem stukje bij beetje te doorgronden, als hij ook gewoon kan vragen om wat hij nodig heeft? Door op het juiste moment de juiste vragen te stellen aan de juiste personen, kan hij relatief eenvoudig informatie verkrijgen. Informatie die op het eerste gezicht misschien onschuldig lijkt, maar die hackers uiteindelijk in staat stelt om zichzelf toegang te verschaffen tot gevoelige bedrijfsgegevens.

Onderzoek toont een groei van social engineering aan, maar in Nederland wordt er nog weinig aandacht aan deze problematiek geschonken. De kans om slachtoffer te worden van een social engineering aanval neemt toe en de financiële schade van een aanval kan aanzienlijk zijn.

Het is dan ook niet voor niets dat Sogeti continu bezig is organisaties bewuster te maken van hun kwetsbaarheid voor Social Engineering. In dat kader organiseerde Sogeti in het voorjaar van 2013 voor de 2e keer de Sogeti Social Engineering Challenge.

In de komende hoofdstukken volgt allereerst een uiteenzetting over de ins en outs van Social Engineering, vervolgens gaan we dieper in op de resultaten van Sogeti Social Engineering Challenge 2013 en sluiten we af met tips voor uw tegenaanval zodat u de stap kunt maken van veilig voelen naar echt veilig zijn.

02

Social Engineering

Social Engineering

Wat is Social Engineering?

Social Engineering is een vorm van 'hacken', waarbij wordt ingespeeld op de maakbaarheid van de mens. Met behulp van Social Engineering worden mensen gemanipuleerd om informatie te verschaffen of acties uit te voeren om het doel van de hacker te bereiken.

Voor een hacker blijkt Social Engineering veelal een effectiever middel te zijn dan alternatieve aanvalstechnieken. Waar hij anders kan worden gehinderd door firewalls en geavanceerde beveiligingsoplossingen, weet hij zich bij de mens juist vaak gesteund door diens vertrouwen, behulpzaamheid en onwetendheid.

In zijn 'Scam School' video's maakt Brian Brushwood duidelijk dat het bij Social Engineering gaat om het bespelen van de menselijke psyche. Daarbij wordt gebruik gemaakt van de volgende vier basisprincipes:

- Autoriteit overtuigt. Door er uit te zien en je te gedragen alsof je ergens thuis hoort, win je gemakkelijk het vertrouwen van mensen. Zeker als je mensen ook nog eens actief benadert en hen vragen stelt, zul je de situatie eenvoudig kunnen controleren.
- Voor wat, hoort wat. Als je iemand iets geeft, zal hij eerder geneigd zijn iets terug te doen voor je.
- Humor wint harten. Als je mensen aan het lachten weet te maken, zullen ze zich op hun gemak voelen bij je.
- Gewoon omdat het zo is. Als je mensen een reden geeft, zullen ze eerder geneigd zijn gehoor te geven aan je verzoek. Het maakt daarbij niet eens uit welke reden je opvoert, zolang er maar een reden is.

"Social Engineer: een uitdagend beroep."
Interview met Marinus Kuivenhoven in BNR Digitaal; klik hier voor het volledige interview

Hoe het werkt

Om een Social Engineering aanval uit te voeren, zal een hacker ervoor zorgen dat hij voldoende informatie over zijn slachtoffer of diens omgeving verzamelt, bijvoorbeeld over diens kennisniveau en interesses. Dit bepaalt de rol en de identiteit die hij aan zal nemen in de interactie met zijn slachtoffer.Daarbij kan hij er bijvoorbeeld voor kiezen in te spelen op de onwetendheid van gebruikers ten aanzien van IT-systemen, door hen te confronteren met technische informatie, die zij moeilijk kunnen bevatten. Gebruikers reageren vaak op bekende meldingen, zoals een slotje in de browser of een melding van een virusscanner. Deze meldingen wekken vertrouwen, terwijl ze door een aanvaller met enige IT-kennis juist gemakkelijk zijn na te maken.

Een hacker kan zijn Social Engineering aanval op verschillende manieren uitvoeren, bijvoorbeeld door middel van 'phishing'. Zo lekte *The New York Times* maandenlang informatie (waarschijnlijk naar China) na een nepmail over een niet geleverd postpakket. Nadat medewerkers op een link in de bewuste mail hadden geklikt, raakte hun computer besmet met kwaadaardige software en kon eenvoudig informatie worden weggesluisd. Met links naar spectaculair nieuws, filmpjes en foto's, via de mail, maar vooral ook op social media zoals Twitter en Facebook, kan eenvoudig hetzelfde effect worden bereikt.

Een andere methode om toegang te krijgen tot bedrijfsinformatie is door fysiek naar binnen te gaan, bijvoorbeeld verkleed als een koerier of onderhoudsmonteur, of door simpelweg met anderen mee te lopen.

Neptelefoontjes van zogenaamde helpdesk medewerkers die slim gebruik maken van gesprekstechnieken, kunnen ook op een eenvoudige manier gevoelige informatie opleveren. Simpelweg door de mensen deze informatie zelf prijs te laten geven of door ze naar een besmette website te dirigeren. Exemplarisch hiervoor was de scamoperatie die Nederland in 2012 geruime tijd in de greep hield, waarbij zogenaamde medewerkers van Microsoft mensen thuis opbelden om ze kwaadaardige software te laten installeren.

Wanneer moet er bij u een belletje gaan rinkelen?

Veelgebruikte methoden om gegevens te stelen

- Phishing, zowel via mail als via social media.
- Neptelefoontjes helpdesk.
- Ransomware (de pc wordt 'gegeijzeld' en vrijgegeven na betaling van een boete).
- Mobiele apps die hengelen naar persoonlijke gegevens, zoals telefoonnummers en accountgegevens.
- Gerichte aanvallen op één gebruiker of organisatie (spear phishing).

10 populairste doelen waar cybercriminelen het op voorzien hebben

- Naam en gebruikersnaam
- Adres en telefoonnummer
- Sofinummer
- Wachtwoord of pincode
- Bankrekening, pasnummer
- Creditcard en validatiecode
- Apple-ID
- Paypal
- Facebook en Twitter
- Gmail, Hotmail

20 meest voorkomende woorden in phishing mails

DHL	Notification	Delivery
Express	2012	Label
Shipment	UPS	International
Parcel	Post	Confirmation
Alert	USPS	Report
Jan2012	April	IDnotification
Ticket	Shipping	

5 meest gebruikte categorieën in kwaadaardige mails

- Post (26,3 %)
- Dringende oproepen (10,7%)
- Bankieren/belastingen (3,8%)
- Vliegreizen (2,5%)
- Rekeningen (0,7%)

Bron: 'Gekraakt door een smoesje' , interview met Sogeti Security Expert Marinus Kuivenhoven in het NRC, 6 april 2013.
Lees hier het volledige artikel.

Waarom het werkt

Mensen zijn zich over het algemeen niet bewust dat er bij henzelf of bij het bedrijf waar ze werken iets te halen is. De informatie waar zij beschikking over hebben, kan aantrekkelijk kan zijn voor een Social Engineer. Zeker als deze uit is op geldelijk gewin of het schade toebrengen aan het bedrijf.

En als ze zich daar al bewust van zijn, dan zijn ze meestal niet voldoende op hun hoede om een Social Engineering aanval te herkennen. Laat staan om deze af te weren.

In hun Comprehensive Study of Social Engineering Based Attacks in India wijzen Chitrey e.a. op twee kwetsbare groepen die in het bijzonder het risico lopen om slachtoffer te worden van een Social Engineering aanval:

- Individuele personen die (nog) niet goed op de hoogte zijn van het beveiligingsbeleid van de organisatie, zoals: nieuwe medewerkers, klanten, partners en extern personeel (contractors).

- Specifieke groepen die toegang hebben tot gevoelige informatie en die tegelijkertijd veel externe contacten onderhouden, zoals: top management en assistenten, HR medewerkers en IT personeel.

Daarnaast geven bedrijven zelf ook onbewust al veel informatie over zichzelf prijs, via openbare websites, sociale media, vacaturesites, etc..

Hoewel dit op zich niet altijd gevoelige informatie hoeft te zijn, kan een hacker met deze informatie, of door een combinatie van deze informatie, wellicht gemakkelijker een andere aanval inzetten. De creativiteit van hackers is wat dat betreft eindeloos.

De gevolgen

In zijn Cybersecuritybeeld Nederland van 2013 wijst het Nationaal Cyber Security Centrum (NCSC) erop dat in het afgelopen jaar de omvang van de criminele cyberdienstverlening aanzienlijk gegroeid is. En in navolging van alle 'cloud' ontwikkelingen doet ook 'cybercrime-as-a-service' zijn intrede.

Omdat criminele organisaties net zo werken als andere bedrijven, is de 'return on investment' van belang.

Aangezien de investeringen voor het doen van Social Engineering aanvallen lager zijn dan die voor andere aanvallen, ligt het voor de hand dat men als eerste naar dit middel grijpt.

De schade die dit oplevert voor getroffenen, kan aanzienlijk zijn. Het NCSC wijst op de primaire bedreigingen bij diverse doelgroepen:

- Overheden: aantasting van de vertrouwelijkheid van informatie en verstoring van de continuïteit van de dienstverlening.

- Bedrijfsleven: verstoring van de continuïteit van de (online) dienstverlening, het weglekken van concurrentiegevoelige informatie en financiële schade.

- 51% van de social engineering aanvallen worden ingegeven door financieel gewin, op de voet gevolgd door toegang tot bedrijfsgeheimen (46%) en/of concurrentiegevoelige informatie (40%).

- Aanvallen doen zich veelvuldig voor: in 32% van de gevallen wordt een frequentie gemeld van 25 of meer aanvallen over een periode van twee jaar.

- In bijna de helft van de gevallen wordt een schade gemeld van meer dan $ 25.000,- per aanval. Bij grotere organisaties is dat zelfs meer dan $ 100.000,- per aanval.

03

Sogeti Social Engineering Challenge 2013

Sogeti Social Engineering Challenge 2013

Doelstelling

Het doel van de Sogeti Social Engineering Challenge 2013 was het onderzoeken in hoeverre grote Nederlandse organisaties kwetsbaar zijn voor Social Engineering.

In 2012 was Sogeti de eerste in Europa die een dergelijk evenement, naar Amerikaans voorbeeld, organiseerde. In april 2013 werd tijdens de Hack-In-The-Box conferentie de aftrap gegeven voor de tweede editie.

Waren Nederlandse organisaties in 2012 nog niet van te voren ingelicht over dit initiatief, voor de editie van 2013 meldde een aantal van hen zich zelfs spontaan aan om een aanval te 'ondergaan'.

Bij het beoordelen van de resultaten is gekeken naar trends in vergelijking met de resultaten van 2012, en naar eventuele verschillen tussen bepaalde bedrijfstakken.

Aanpak

Voor de editie 2013 hadden zich 12 deelnemers aangemeld en in totaal zijn 25 willekeurige bedrijven uit de Nederlandse top 100 onderzocht. Ook Sogeti zelf werd gechallenged.

De challenge was zo opgezet dat deze binnen de kaders van wet- en regelgeving viel. De deelnemende 'hackers' moesten zich daarom aan strikte regels houden. Het doel was immers niet om bedrijven lastig te vallen, vertrouwelijke informatie te bemachtigen of in een kwaad daglicht te stellen. De deelnemers kregen vooraf één of enkele bedrijven toegewezen, waarover zij een voorgeschreven set aan informatie moesten zien te vergaren (zie kader). Daarbij mocht alleen gebruik gemaakt worden van openbare bronnen, zoals zoekmachines en de website(s) van de bedrijven zelf.

De feitelijke Challenge bestond uit het voeren van één of meer telefoongesprekken. Andere vormen van het benaderen van de bedrijven waren niet toegestaan. Tijdens de Challenge werden in totaal 53 telefoontjes gepleegd.

Voorbereiding

Opvallend was dat tijdens de voorbereidingsfase bij verschillende bedrijven al veel (vaak ook gevoelige) informatie te verkrijgen was, gewoon uit openbare bronnen.

De zoekmachine van Google was daarbij het belangrijkste hulpmiddel. Uit publicaties van de bedrijven zelf kon soms al het nodige worden afgeleid, hetzij door de inhoud van deze documenten, foto's of presentaties, hetzij via de documenteigenschappen. Zo kon bijvoorbeeld aan de hand daarvan de versie van de gebruikte software worden achterhaald maar ook de naam van de auteur van het document.

Te verkrijgen informatie

- Welke typen en versies gebruikt het bedrijf van de volgende software: operating systeem, internet browser, e-mail client en pdf-reader?
- Wat is de URL van het intranet?
- Wat is de naam van het interne draadloze netwerk?
- Wat zijn de namen van de volgende dienstverleners van het bedrijf: cateraar, fysieke beveiliger, archiefvernietiger en IT-serviceorganisatie?

Uit te voeren acties

- Registreer jezelf als bezoeker.
- Laat je slachtoffer een website openen met een flash of .pdf bestand.

Sociale media volgden als goede tweede informatiebron. LinkedIn bleek bijvoorbeeld veel nuttige informatie te bevatten over de structuur van bedrijven en ook namen van personeelsleden en hun functies waren hier te vinden. In een enkel geval konden op Twitter ook nog eens foto's worden verkregen van de werkplekken van medewerkers.

Eén van de deelnemers trof op Slideshare zelfs een complete back-up aan van interne presentaties van het bedrijf dat hij moest aanvallen.

Ook op vacaturesites kon de nodige informatie verzameld worden. Dat gold o.a. voor de vacatureteksten, waarin soms heel gedetailleerde informatie werd gegeven (bijvoorbeeld: "Wij zijn op zoek naar een Oracle 10G Release 2 specialist voor een intern migratietraject"). Aan de hand van dergelijke specifieke informatie kan een aanvaller bijvoorbeeld kijken of er kwetsbaarheden bekend zijn voor de betreffende versie van de software. Daarnaast vormden ook de beschrijvingen van werkzaamheden en vaardigheden in de CV's van (ex-) medewerkers een belangrijke bron van informatie.

Challenge

De drie belangrijkste groepen 'slachtoffers' betroffen: de receptie, de IT-servicedesk en recruiters. Deze nummers waren namelijk het gemakkelijkst te vinden.

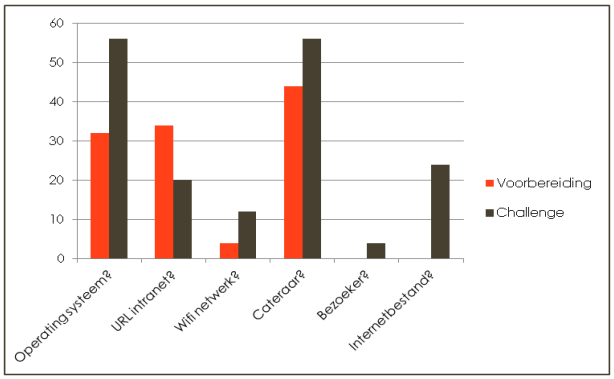
Op basis van de informatie uit de voorbereidingsfase hadden alle deelnemers hun verhaal (smoes) klaar, waarmee zij hun 'slachtoffers' aan het praten probeerden te krijgen. In Social Engineering termen wordt dit de 'pre-text' genoemd.

De meest gebruikte 'pre-texts' waren die, waarin de deelnemer een plausibele reden opgaf waarom hij de informatie nodig had:

- De student/onderzoeker die informatie nodig heeft voor zijn scriptie/onderzoek over een onderwerp.

- De potentieel toekomstige medewerker die meer informatie wil over het bedrijf waar hij komt te werken.

Het schema hierna bevat een beknopt overzicht van het totaal resultaat van de Sogeti Social Engineering Challenge 2013. De rode staaf geeft aan in hoeverre de informatie tijdens de voorbereidingsfase is verkregen, terwijl de grijze staaf representatief is voor de verkregen informatie tijdens de telefoongesprekken. Hierbij geldt: hoe hoger de 'score', des te slechter de prestatie.



Figuur 1 – Beknopte weergave resultaten Challenge 2013

Access.
Je gebruikt deze informatie toch niet om te hacken hè?
Granted.

Enkele opvallende constateringen

- In meer dan de helft van de gevallen kon informatie worden verkregen over de gebruikte software (operating systeem) en de gebruikte versies daarvan. Zeker wanneer nog gebruik gemaakt wordt van oudere versies, maakt dit bedrijven kwetsbaar. Voor oudere versies zijn namelijk volop kwetsbaarheden bekend en aanvalsmethoden aanwezig.

- Bij ruim 30% van de bedrijven kon de URL van het intranet worden achterhaald. Daarmee kan worden geprobeerd op het intranet te komen en daar informatie af te halen of om verder in het netwerk te komen. De ervaring leert dat er voor een intranet minder beveiligingsmaatregelen getroffen worden, dan voor een externe website. Informatie van het intranet stelt een hacker in staat om gebruik te maken van 'vakjargon' van het bedrijf in kwestie en wint daardoor eerder het vertrouwen van de mensen die hij benadert.

- Informatie over het Wifi-netwerk kon binnen de richtlijnen van de Challenge slechts beperkt worden achterhaald. De kans is namelijk groot, dat wanneer je je auto in de buurt van het bedrijf zou parkeren, deze informatie wel te vinden zou zijn. De bedreiging die hiervan uit gaat, is dat een hacker een Wifi-netwerk aan kan maken, dat technisch lijkt op het netwerk van het bedrijf. Wanneer een laptop of mobiel apparaat automatisch verbindt met een 'bekend' netwerk, kan deze zich ook met het nagebootste netwerk verbinden, waarna de aanvaller alle verkeer kan afluisteren (een zogenaamde 'Man-in-the-Middle' aanval).

- Informatie over de diverse dienstverleners van een bedrijf, zoals de cateraar, was ook in een groot aantal gevallen eenvoudig te achterhalen. Een aanvaller die de dienstverleners van een bedrijf kent, kan vervolgens 'namens' deze dienstverleners fysiek langs gaan bij het bedrijf, of verzoeken aan gebruikers doen.

- Tijdens de Challenge lukte het slechts 1 deelnemer om zichzelf geregistreerd te krijgen als bezoeker. Het gevaar dat daarin schuilt, is dat een hacker hiermee 'legitiem' fysieke toegang tot het pand krijgt. Hij kan dan bijvoorbeeld iets in het pand achter laten, waarmee hij van buitenaf verbinding met het bedrijfsnetwerk houdt.

- In ruim 20% van de gevallen lukte het om het slachtoffer een website en/of een bestand op internet te laten openen. Hiermee kan een aanval ingezet worden doordat het geopende bestand (Flash, website of PDF) de mogelijkheid biedt om misbruik te maken van veiligheidsgaten in verouderde/kwetsbare software. De hacker heeft daarvoor alleen een geautoriseerde gebruiker nodig.

Bedrijven publiceren veel informatie over zichzelf op openbare websites. Vanuit een bedrijfsdoel is dit een logische stap. Voor een Social Engineer zeer waardevolle informatie om zijn aanval effectiever te maken.

Medewerkers van organisaties bleken tijdens de Challenge over het algemeen bereidwillig bij het verstrekken van de gewenste informatie, ongeacht of dit wel logisch was vanuit hun rol.

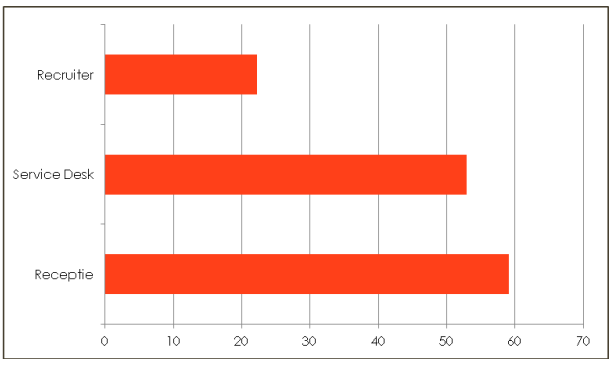
Complimenten geven

De techniek die daarbij goed werkte was (subtiele) vleierij. Het geven van complimenten werd goed ontvangen en hielp in een aantal gevallen duidelijk om , waar een gesprek eerst nog wat moeizaam verliep, het gesprek open te breken. Ook het bewust maken van een vergissing of het laten vallen van stiltes bleek effectief te zijn. Waar een deelnemer aan de Challenge begon met 'jullie cateraar is toch ...', werd dit door het 'slachtoffer' plichtsgetrouw verbeterd dan wel ingevuld.

Vragen werden door medewerkers zoveel mogelijk beantwoord en als men het even niet wist, werden instructies voor het achterhalen van de informatie gewillig opgevolgd. In deze gesprekken was het gebrek aan IT-kennis of de beperking in systeemrechten vaak de beperkende factor om meer aan de weet te komen. Hieruit blijkt eens te meer dat mensen het moeilijk vinden om 'nee' te zeggen!

Weerstand

Ten opzichte van de Sogeti Social Engineering Challenge van 2012 bleek er wel een duidelijk verschil waarneembaar bij de benadering van receptiemedewerkers, die meer blijk gaven van een wat kritischer houding. Enerzijds was men heel expliciet: men mocht of kon geen antwoord op de vraag geven. In andere gevallen werd er eerst met ene collega overlegd in hoeverre er antwoord gegeven mocht worden. Ook het advies om maar een e-mail te sturen, zodat de vragen 'bij de juiste persoon terecht konden komen' bracht de deelnemers niet verder bij hun doel. Het volgende schema geeft per groep 'slachtoffers' aan in welk percentage van de gesprekken weerstand te merken was.



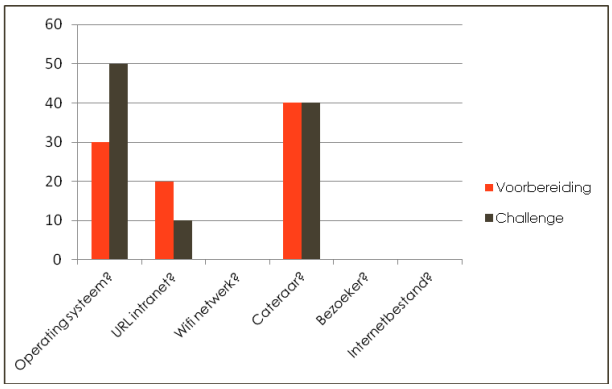
Figuur 2 - Percentage waarbij weerstand te merken was.

Bedrijfstakken

Naast het totaalresultaat hebben we ook gekeken naar de resultaten binnen de drie belangrijkste bedrijfstakken die tijdens de Challenge zijn onderzocht:

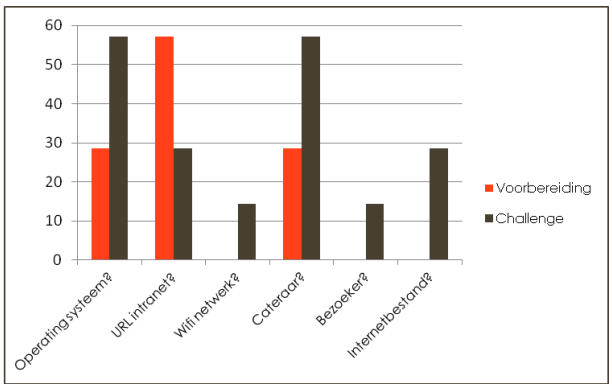
- Handel en industrie
- Zakelijke dienstverlening
- Financiële dienstverlening

Onderstaande schema's geven een beeld van de resultaten per bedrijfstak. Ook hierbij geldt: hoe hoger de 'score', des te slechter de prestatie van de organisatie op het gebied van Security.



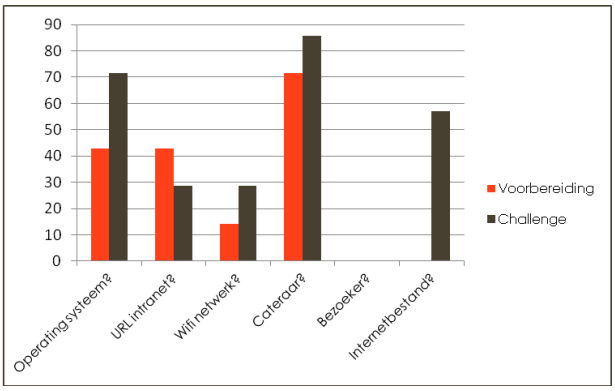
Figuur 3 - Resultaten Handel en Industrie

De relatief goede resultaten bij Handel en Industrie zijn voor een belangrijk deel te verklaren doordat het in deze bedrijfstak moeilijker was om voorbij de receptie te komen. Ook waren telefoonnummers van bijvoorbeeld de receptie of een servicedesk moeilijker te achterhalen.



Figuur 4 - Resultaten Zakelijke dienstverlening

De resultaten bij bedrijven in de zakelijke dienstverlening zijn iets vertekend. Bij enkele bedrijven kon bijna geen informatie verkregen worden; bij andere bedrijven in deze categorie werd juist heel veel informatie achterhaald.



Figuur 5 – Resultaten Financiële dienstverlening

De Financiële dienstverleners scoorden duidelijk het slechtst in de Challenge van 2013. Een opmerkelijke uitkomst als we bedenken dat juist financiële instellingen veelvuldig het doelwit van aanvallen zijn geweest en de verwachting is dat dit alleen nog maar toe zal nemen.

Alleen al vanwege het feit dat het achterhalen van gevoelige gegevens bij een financiële instelling al snel leidt tot financieel gewin voor een kwaadwillende hacker, zijn financiële instellingen een aantrekkelijk doelwit.

Damage.
Kun je de deur even voor me openhouden?
Ik ben mijn pasje vergeten.
Control.

04

Conclusie

Conclusie

Factor Mens onderschat

Hoewel de technische beveiliging bij veel van de onderzochte bedrijven wel op orde is, toont Sogeti's Social Engineering Challenge 2013 weer aan dat de factor mens nog vaak onderschat wordt.

Een Social Engineer die de goede antwoorden klaar heeft en thuis is in het bespelen van de menselijke psyche, kan heel ver komen.

Iedere deelnemer is het gelukt om meerdere onderdelen van de gevraagde informatie te achterhalen. Geen van de bedrijven hing op en slechts in beperkte mate kreeg de deelnemer te horen dat informatie niet toegankelijk was.

Ook deelnemers met relatief weinig voorbereiding en/of weinig Social Engineering ervaring kregen bedrijfsinformatie in handen die in eerste instantie misschien onschuldig leek, maar wel degelijk inzetbaar is voor een meer gerichte aanval.

Belangrijke informatie vrij toegankelijk

Bedrijven en hun medewerkers zijn zich nog onvoldoende bewust van het feit dat zij via openbare websites en social media veel bedrijfsinformatie prijsgeven.

Met relatief weinig voorbereiding en in korte tijd kon daardoor binnen de beperkte context van de Social Engineering Challenge op simpele wijze veel informatie achterhaald worden. Het is dan ook zeker niet ondenkbaar dat in grootschaliger opgezette aanvallen alle gewenste informatie kan worden gevonden.

Hoewel het in het openbaar publiceren van bedrijfsinformatie in veel gevallen een bewuste keuze is, hebben wij sterk de indruk dat bedrijven onvoldoende op de hoogte zijn van de kwetsbaarheden op dit gebied.

Verschillen tussen branches

Van de onderzochte branches bleken met name de financiële dienstverleners kwetsbaar voor Social Engineering aanvallen. Een zorgelijke constatering, aangezien zij toch al vaak het doelwit van allerlei security-aanvallen zijn.

Gelet op het grote belang van de door de financiële instellingen aangeboden e-banking- en e-finance-dienstenen de noodzaak om het vertrouwen van het publiek in deze diensten te vrijwaren, hadden we verwacht dat we meer Security Awareness bij de benaderde medewerkers zouden ondervinden tijdens het onderzoek. Uit onze ervaring als dienstverlener bij diverse financiële intstellingen weten we dat de meeste grote banken en verzekeraars hun eigen security teams hebben die technisch gezien de security van de bank/verzekeraar borgen. Ook zijn er vaak GRC (Governance, Risk & Compliance)-teams ingezet die business processen, security maatregelen, beleid en verandertrajecten toetsen aan diverse normenkaders, zoals die van de DNB, of bijvoorbeeld ISO27001 of Cobit.

Maar wie zorgt er nu voor de zwakste schakel in de security: de servicegerichte medewerker?

Belangrijkste redenen om te investeren in Security

- Verlaging TCO
- Kostenbesparing incidentoplossing
- Continuïteit van core business
- Beperken gevolgschade

De tegenaanval

Zoals uit dit rapport blijkt, kent Social Engineering verschillende verschijningsvormen. Wat heeft u nodig om uw bedrijf weerbaarder te maken en de tegenaanval in te zetten?

Security Awareness

Veruit de belangrijkste manier om Social Engineering tegen te gaan is Security Awareness.

Programma's voor bewustwording, opleidingen en trainingen moeten ervoor zorgen dat mensen Social Engineering herkennen en zich bewust zijn van de impact en hun rol daarin. De programma's zijn dan zowel gericht op medewerkers in het algemeen als specifieke (kwetsbare) groepen in het bijzonder,

Werknemers moeten leren mogelijke aanvallen te herkennen. Anderzijds moeten ze weten hoe hierop te reageren. Zo moeten ze bijvoorbeeld leren meer vanuit hun eigen 'rol' te denken: 'Wat is vanuit mijn positie logische informatie om te verstrekken en wat niet?'. Ook moeten ze op de hoogte worden gebracht van de procedures voor het melden van incidenten.

De kracht zit in de herhaling: dergelijke bewustwordingsprogramma's moeten regelmatig worden herhaald.

"Mensen mogen best 'Nee' zeggen."

Ervaringsleren heeft in deze een groter effect. Buiten de grenzen van de reguliere ''klaslokaal'-opzet werkt een spelelement zeer effectief. Geef medewerkers bijvoorbeeld de mogelijkheid om een maand lang het bedrijfspand binnen te komen, maar dan niet op de normale manier. Als ze dat lukt, krijgen ze punten en degene die aan het einde de meeste punten heeft verzameld, krijgt een 'prijs'. Omdat niet iedereen zich aangetrokken zal voelen om hieraan mee te doen, kunnen ze ook punten verdienen als ze een zwakke plek alleen al kunnen detecteren. Hiermee kunnen niet alleen nog niet bekende zwakheden in kaart gebracht worden, maar kan ook de betrokkenheid van de medewerkers aanzienlijk vergroot worden.

Fysieke beveiliging

Bewustwording alleen zal niet voldoende zijn om alle Social Engineering aanvallen het hoofd te bieden. Aanvullende maatregelen, bijvoorbeeld op het gebied van optimale fysieke beveiliging, zullen daarom zeker overwogen moeten worden.

Denk daarbij een sluitend systeem van toegangscontroles, bewaking en monitoring, het afschermen van kwetsbare ruimten en een gecontroleerde afvoer en vernietiging van gevoelig materiaal.

Technische beveiligingsmaatregelen

Voorbeelden van technische beveiligingsmaatregelen zijn: de toepassing van sterkere authenticatie bij de toegang tot gevoelige informatie (bijvoorbeeld niet alleen een wachtwoord, maar ook een PIN-code) en het blokkeren van buitenlandse telefoongesprekken.

Beveiligingsbeleid

Het voeren van een eenduidig beveiligingsbeleid – met duidelijke do's en don'ts, gedragscodes en sancties is essentieel in het afweren van Social Engineering aanvallen.

Inzet van één of een combinatie van deze middelen brengt u 'van veilig voelen naar echt veilig zijn'.

Tips voor medewerkers

- **Blijf kritisch en alert**
  Laat je niet overrompelen door mooie praatjes.
- **Blijf in je rol**
  Laat je niet verleiden tot het geven van informatie die niet bij je rol/functie past
- **Houd anderen alert**
  Beveiliging is een gezamenlijke verantwoordelijkheid. Spreek dus een collega aan wanneer je ziet dat hij onzorgvuldig omgaat met informatie.

05

Over Sogeti

Over Sogeti

Passie voor ICT

Sogeti is gespecialiseerd in het ontwerpen, bouwen, implementeren en beheren van ICT-oplossingen. Op het gebied van testen en architectuur nemen wij op de Nederlandse markt een dominante positie in. Sogeti levert met gepassioneerd ICT-vakmanschap een bijdrage aan het resultaat van haar opdrachtgevers. Wij streven daarbij naar hechte en langdurige relaties met opdrachtgevers. Hierdoor dragen de ICT-oplossingen van Sogeti structureel bij aan de strategische doelstellingen van klanten.

Op risico gebaseerde aanpak

Omdat uw bedrijf doorlopend verandert om in te spelen op de marktvraag, verandert ook uw ICT-landschap continu. Daarnaast hebben bijvoorbeeld Bring Your Own Device, Mobile, uw websites, klantportalen en Big Data een grote impact op uw strategie. En daardoor security ook.

Sogeti onderzoekt hoe veilig uw ICT-systemen zijn. We helpen u om security te integreren in uw organisatie en om adequaat te reageren op steeds nieuwe securityrisico's. Zo kunt u veilig uw businessdoelstellingen halen.

Wij bieden een op risico gebaseerde security visie. Deze visie, de Proactive Security Strategy (PaSS®), rust op drie pijlers: organisatie, infrastructuur en software en vindt zijn oorsprong in een belangrijk doel: van veilig voelen naar veilig zijn.

Met onze aanpak verhoogt u de efficiency van uw (ICT-)veranderingsproces en bespaart u veel kosten.
U bent in control, uw organisatie opereert efficiënter en is veilig.

Sogeti Security maakt het verschil

In plaats van te reageren op incidenten, zorgt Sogeti voor proactief passende security-maatregelen. We bieden een compleet dienstenpakket met oplossingen die gericht zijn op het identificeren, verminderen en voorkomen van security-risico's.

Onze resultaten

- Organisaties hebben inzicht in risico's en kwetsbaarheden van hun systemen door Security Testing, zoals Penetratie- en Vulnerability-testen.
- Na implementatie van onder andere ISO 27001-beleid en -maatregelen worden succesvolle pre- en post-audits uitgevoerd.
- Bedrijven maken de stap naar de cloud en hun Identity&Accessmanagement is goed ingericht.
- Met Security Information and Event Management (SIEM) monitoren we de IT-infrastructuur,verminderen security-incidenten en is er altijd real-time inzicht in mogelijke risico's.
- Awareness programma's en trainingen zorgen voor bewustwording van medewerkers over hun rol en verantwoordelijkheid in informatiebeveiliging.

Kortom, organisaties zijn in control over hun security. Ze kunnen op basis van afgewogen risico's keuzes maken over hoe zij hun business doelen kunnen bereiken.

Meer informatie over Sogeti is te vinden op **sogeti.nl/security** of neem contact met ons op via **security@sogeti.nl**.

Je kunt ons ook googlen, bel gewoon de receptie of klik hier.

Doet u mee aan de Sogeti Social Engineering Challenge 2014?

Sogeti Nederland B.V.
Postbus 76
4130 EB Vianen
sogeti.nl/security
security@sogeti.nl