

Social engineering kan veiligheidsbewustzijn vergroten

Security: niet mijn pakkie-an

Als het om beveiliging van informatie gaat, is de technische kennis veelal wel voorhanden. Ook organisatorisch weten de meeste ondernemingen en instellingen inmiddels – al dan niet geholpen door externe factoren als normen en wetten – wat ze wel en niet willen. De factor ‘mens’ vormt echter een probleem dat steeds meer onder de aandacht komt: de mentaliteit van ‘niet mijn pakkie-an’ moet worden omgevormd naar ‘wel degelijk (ook) mijn probleem’. Hans Labruyère, die zich beroepsmatig met social engineering bezighoudt, betoogt dat deze discipline hierbij behulpzaam kan zijn.

Hans Labruyère

Ik stap in de lift van een gebouw van een grote organisatie, en druk op de knop van de zevende verdieping. Op de tweede houdt de lift stil. Twee dames stappen al babbelend in. De ene vertelt aan de andere dat ze een weekje naar een zonnig eiland gaat. Dat is leuk, vindt ook de ander, “... maar ik wil wel graag in het dossier van firma x en meneer y kunnen. Hoe doen we dat dan?” Het antwoord is even simpel als ongelooflijk: “Ik geef je mijn password wel even. Heb je een pen?” Ik heb wél een pen. En nog drie verdiepingen om de gegevens op te schrijven. “Tja,” lacht de tweede dame tegen mij, “dan moeten ‘ze’ maar zorgen dat ik in haar systeem kan als ze op vakantie is. Niet mijn pakkie-an!” Ziehier een voorbeeld van hoe het niet moet maar hoe het wel vaak gaat. Bij gesprekken met opdrachtgevers wordt over het algemeen begripvol geknikt bij het aanhalen van een wat ouder KPMG-rapport (2003), dat onder andere aangaf dat zeventig procent van de incidenten binnen informatiebeveiliging helemaal niet ‘van buiten komt’ – en ook lang niet altijd opzettelijk van aard is.

Nut en noodzaak

Informatie is voor elke organisatie van levensbelang. Informatie dient integer, betrouwbaar, vertrouwelijk en beschikbaar te zijn. En voor de goede orde: die informatie is lang niet altijd digitaal. Veel, heel veel informatie wordt

‘gewoon’ nog op papier verwerkt. En denk eens aan de kennis die in de hoofden van de medewerkers zit. Het loont de moeite eens serieus met alle betrokkenen na te denken over het nut en de noodzaak van informatiebeveiliging. En de uitkomst van zo’n analyse kan heel goed zijn dat informatiebeveiliging op bepaalde bedrijfsonderdelen niet nuttig of noodzakelijk is. Maar dat is dan is wel een bewust ‘nee’. Vandaag de dag is het antwoord op de vraag of men aan informatiebeveiliging doet, vaak: “Nee, want wij worden niet gehackt.” Terwijl men eigenlijk bedoelt: “We denken dat het niet gebeurt, want we zien het niet.” Denk eens aan uw eigen organisatie, uw eigen plek in het geheel: hoe vaak hebt u uw bestuur tevergeefs ervan proberen te overtuigen dat een bepaalde investering of procedure absoluut noodzakelijk is, terwijl het bestuur daar heel anders over dacht?

Bewustzijn kweken

Dus wat te doen als de afdeling IT wel degelijk beseft dat de status van beveiliging niet op alle punten voldoende is maar de rest van de organisatie daar heel anders over denkt (‘niet mijn pakkie-an’)? In dat geval kan het helpen als zich een incident voordoet. Maar die IT-afdeling zit natuurlijk niet te wachten op een incident: de kans is groot dat zij (in ieder geval een deel van) de schuld krijgt.

Mystery guest – 1

Een *mystery guest* (een ingehuurde social engineer die de beveiliging aan de tand komt voelen) treft in een bedrijfspand een laptop aan die niet aan een kabel is vastgelegd. Bij zijn vertrek vraagt de receptioniste hem vriendelijk of hij een uitvoerbewijsje of de naam van een begeleider kan overleggen voor de machine onder zijn arm. Hulde voor de mevrouw in kwestie! Hack mislukt, althans in eerste instantie. Na de pauze is er echter een wisseling van de wacht bij de receptie, en inmiddels heeft de *mystery guest* zes laptops verzameld. De nieuwe receptioniste doet de deur gewoon open voor de *mystery guest*, mompelend "het zal wel zwaar zijn".

De ernst van dit voorbeeld zit hem niet primair in die zes maal twee mille, maar vooral in het gemak waarmee wordt omgegaan met de data die op de laptops staan.

Bovendien doet zo'n incident zich altijd voor als het niet uitkomt.

Daarom zijn er *vooropgezette* incidenten in het leven geroepen (zie voorbeelden in kaders 'Mystery guest'), die die nadelen niet kennen: dan heeft men oorzaak en gevolg tot op zekere hoogte in de hand, en kan men zich volledig richten op de resultaten van wat er is gebeurd. Dit soort incidenten kunt u heel goed zelf uitvoeren. Dat heeft als voordeel dat u de manier, het moment en de schaal waarop ze voorkomen, vooraf zelf kunt bepalen. Bij een dergelijk incident wordt de medewerkers niet alleen getoond dat het kan gebeuren, maar vooral dat het ook hún kan overkomen. Dit brengt een bewustwordingsproces teweeg waarbij de medewerkers de geconstateerde situatie in verband gaan brengen met hun eigen rol hierin.

De Amerikaanse wetenschapper Maslow zei het al: als men in staat is een bepaald onderwerp terug te brengen tot individueel niveau (het menselijk basale niveau waarop vragen worden gesteld als: 'heb ik vandaag te eten?' en: 'hebben mijn kinderen een dak boven het hoofd?') maakt men veel meer kans een

bewustwordingscampagne succesvol af te sluiten. Dus het gaat dan niet om bewustwording op corporate niveau, want dan is het onderwerp helemaal 'ver van ieders bed'. En ook het afdelingsniveau is geen goede scope, want dan is er altijd wel een collega of afdelingschef die (een deel van) de schuld kan krijgen. Succes in informatiebeveiliging is vooral afhankelijk van de bewustwording van iedere afzonderlijke medewerker: denk *jij* maar eens na over de informatie waar *jij* toegang toe hebt. En hoe ga *jij* om met de bescherming van die gegevens? En wie (of wat) zou *jou* kunnen bedreigen, al dan niet met opzet? En hoe zou *jij* daar maatregelen voor kunnen nemen? Of wie zou je daarvoor nodig kunnen hebben?

Op die manier creëert de organisatie een draagvlak op individueel niveau. Daardoor zullen gestelde regels beter worden begrepen en in de praktijk betere resultaten kunnen hebben.

Beveiliging van informatie wordt iets van onszelf – en dus noodzakelijk – in plaats van dat het iets 'van de baas' is – en dus lastig. Ook heeft dit collectieve draagvlak tot gevolg dat achterblijvers in dit proces een goede reden krijgen om zich aan te sluiten bij hun collega's: mensen zijn groepswezens en dus wil niemand een uitzondering zijn.

Bovendien kan de betrokkenen na verloop van tijd op eenvoudige wijze worden duidelijk gemaakt dat het beveiligingsniveau daadwerkelijk verbeterd is – aan de hand van (deel)uitslagen van enquêtes, testen en audits. Het gevoel dat hierbij zal optreden, in combinatie met de gedachte dat 'het eigenlijk helemaal niet veel moeite kostte' zal alleen maar positief bijdragen aan het vervolg van het proces. Men zal zich bij een nieuwe verandering in de regelgeving met betrekking tot informatiebeveiliging herinneren hoe weinig moeite het kostte om de organisatie tevreden te stellen en toch het juiste resultaat te bereiken. En bedenk: deze methodiek werkt in de praktijk voor eindgebruikers even goed als voor de twee andere doelgroepen binnen informatiebeveiliging: het management en de 'technisch betrokkenen' zoals IT-medewerkers, beveiligingsmensen, et cetera. Natuurlijk is commitment van het management noodzakelijk voor een goed verloop van het (informatie)beveiligingsproces, maar voor dat commitment moet er eerst bewustzijn worden gecreëerd; anders komt het onderwerp domweg niet op de agenda.

Belachelijk eenvoudig

Als er niet voldoende bewustzijn is bij bijvoorbeeld de Raad van Bestuur of de budgethouder kan het dus vaak helpen om een klein incident te laten optreden. De impact van zo'n vooropgezet incident

SOCIAL ENGINEERING VAN ALLE TIJDEN...



Mystery guest - 2

Bij een mystery guest-actie wordt de social engineers verzekerd dat ze in het hoofdgebouw niet hoeven te acteren, want dat zou zwaar beveiligd zijn. Uiteraard dringen ze toch het gebouw binnen. Ten bewijze hiervan slagen ze erin een foto te maken van de directeur achter zijn bureau, vriendelijk glimlachend. Hij vraagt niet waar de foto voor is, maar treft die later aan op de rapportage van het hackteam. Nadat de hack aan hem uitgelegd is, beseft hij wat de hackers verder nog hadden kunnen doen, voordat de foto gemaakt was.

is er niet minder om: slechts in kleine kring is bekend dat het om een *fake*-incident gaat ...

Het inhuren van een hacker is heel gebruikelijk: soms een buurjongen met goede wil, soms een professionele specialist. Die aanvaller doet het zijne (of hare – vlak de dames niet uit in dit verband) om te zien wat de status van beveiliging van het systeem is. Daarbij kan een antwoord worden gevonden op vragen als: hoe veilig is onze fysieke organisatie? Hoe veilig is dat pasjessysteem eigenlijk? Wat zou iemand kunnen doen die binnen is – en als hij binnen is, zouden wij dat dan zien? Zouden medewerkers iemand aanspreken die ze niet kennen maar die zich wel op hun verdieping ophoudt? Of zou men toch denken: ‘niet mijn pakkie-an’? Of: ‘we hebben een pasjessysteem en hij is binnen, dus hij zal hier wel horen’?

Door middel van social engineering is vaak belachelijk eenvoudig resultaat te bereiken. Mensen zijn dienstbaar: ze helpen je graag aan de gegevens, als je het maar vriendelijk vraagt. Weinig mensen beseffen wat de waarde is van de informatie waar zij op dat moment de beschikking over hebben. Laat staan dat ze zich afvragen of ‘die vent’ werkelijk degene die hij zegt te zijn (verifiëren). En of ze hier wel op mogen antwoorden (controleren). En of het protocol dat wel toelaat (kennis van de procedures)?

En denk niet dat dit soort fysieke veiligheid niet uw probleem is. Want realiseert u zich eens hoe weinig moeite het kost om een wifi-elementje te plaatsen in die openstaande poort in de vergaderkamer. Of welke informatie er nou precies op uw PDA en uw telefoon staat. En waar blijven die apparaten als u een meeting hebt?

In de praktijk

Een aanval van social engineering is goed te combineren met een ethische hack.

Een zogenaamde *mystery guest* (een daartoe ingehuurde social engineer die de beveiliging aan de tand komt voelen – zie de kaders) kan de hacker vaak helpen bij zijn pogingen informatie boven water te krijgen, en op die manier de kwetsbaarheid van de organisatie aan de dag leggen.

Vooropgezette incidenten hebben als voordeel dat de manier, het moment en de schaal waarop ze voorkomen, vooraf te bepalen zijn

Telefonische kwetsbaarheid biedt ook een goede toegangsmogelijkheid. Een medewerker (een niet-IT'er) wordt gebeld door iemand die zich voordoet als een nieuwe helpdeskcollega, die vraagt of de medewerker even opnieuw wil inloggen. Vervolgens geeft die ‘helpdeskman’ aan dat ie onvoldoende kan ‘zien’, en vraagt of de medewerker nogmaals wil inloggen. Een simpele manier om username-passwordcombinaties boven water te krijgen.

Een ander voorbeeld. De hacker is bij de klant binnengelaten, en zit in een vergaderzaal. De contactpersoon weet ervan, en laat zich niet zien. Van internet heeft de hacker vooraf een interne telefoonlijst gedownload, zodat hij met zijn gsm naar de secretaresse van de verdieping kan bellen: “Ja, met Van Santen (lid raad van bestuur, zie internet), ik heb een bespreking met de heer y. Hij zit te wachten in

vergaderzaal z, maar ik ben verlaat. Geef hem even een kop koffie en vraag of je iets voor hem kunt doen. Het duurt nog wel een uurtje. Misschien kun je hem een werkplek geven voor dat uur? Dan kan hij nog wat doen.” Vijf minuten later komt een juffrouw vragen of de man in de vergaderruimte misschien mijnheer y is: “De heer Van Santen laat zich verontschuldigen, maar wilt u misschien even gebruikmaken van een werkplek?” In de praktijk kan deze hacker vervolgens een paar uur op het interne netwerk van de organisatie werken.

De attitude en de boodschap

Als er bewustzijn gekweekt is, is attitudewijziging de volgende stap. Dit blijkt de bottleneck in de meeste informatiebeveiligingsprocessen. Het onderwerp wordt vaak aangevat onder lichte externe dwang: SOX, ISO, NEN 7510, Suwinet, GBA of de accountant geven aan dat er nu toch echt iets moet gebeuren. Een beleid is snel opgesteld, een proceseigenaar is eenvoudig aangewezen – over tot de orde van de dag! Maar zo werkt het natuurlijk niet.

Hoe kan de attitude van medewerkers dan wel veranderd worden? Dwang is een mogelijkheid, maar is gezien de Nederlandse neiging tot revolte wellicht niet de beste optie. Angst is altijd een slechte raadgever, dus ook dat is geen goed middel. Laten we eens kijken naar andere markten met een vergelijkbaar probleem. Elke *fmcg*-fabrikant (*fast moving consumer goods*: voeding, zeepmiddelen, et cetera) zal kunnen bevestigen dat groepsattitude best te sturen is. Buiten een duidelijke boodschap zijn daar maar drie dingen voor nodig: herhaling, herhaling en herhaling.

Hoe is het eigenlijk met de beveiligingsboodschap in uw organisatie? Is die ook helder gesteld? En gericht op het individu? En kent uw organisatie die boodschap eigenlijk wel? Weet zij eigenlijk wat het startpunt – de huidige situatie – is en waar ze naartoe zou (moeten) wil-



security

len? Deze vragen zijn tamelijk generiek voor veel organisaties, en de antwoorden zijn tot op zekere hoogte vaak relatief eenvoudig vast te stellen.

Zelf doen of uitbesteden?

Informatiebeveiliging is primair een zaak van de onderneming zelf; men wil zo veel mogelijk zelf doen. De onderneming zou echter kunnen besluiten sommige dingen uit te besteden aan of samen te doen met een ervaren persoon. Gezamenlijk kunt u bijvoorbeeld een nulmeting houden ten aanzien van bewustwording. Idealiter doet u dit bij verschillende doelgroepen: eindgebruikers hebben een ander zicht op de wereld dan managers. Technische betrokkenen kennen vaak meer relevante details dan leden van de raad van bestuur. Maar ze

zijn allemaal onderdeel van de organisatie en dus is ieders attitude van belang. Na de nulmeting bepaalt u welk gat er zit tussen de feitelijke situatie en de wenselijke situatie. Daarna rolt u een actieplan uit.

Gefundeerde maatregelen

Dit soort aanvallen moet zeker gepresenteerd worden aan (ten minste) de raad van bestuur; het commitment voor informatiebeveiliging moet immers daarvan komen. Die presentaties zijn zonder uitzondering een feest! Ontgoocheling en pret zijn de onderdelen die zulke presentaties compleet maken, maar de serieuze ondertoon van het onderwerp blijft wel vooropstaan. Want pas als het MT of de raad van bestuur zich de ernst van de zaak realiseert, mag je verwachten dat

het maatregelen zal nemen – ook op het gebied van IT.

En dan graag gefundeerde maatregelen, gebaseerd op weloverwogen risicoanalyses. En niet, zoals nu vaak het geval is, op basis van een ruwe schatting van een goed bedoelende betrokkene, die vaak ook niet het hele veld kan overzien. Want als zich incidenten beginnen voor te doen, wordt die goed bedoelende betrokkene er als eerste met de haren bij gesleept om uit te leggen hoe dit nu toch allemaal kon gebeuren. En dan is het te laat om aan te komen met: “Ja maar u had ook nooit aandacht voor mijn problemen.” Niet mijn pakkie-an, weet u nog wel.