Sociale media: valkuilen en voordelen

Door: Raoul van Boekholdt

De afgelopen jaren zijn sociale media als paddenstoelen uit de grond geschoten en hebben zij een ongekende groei doorgemaakt. Ze hebben tegenwoordig een vaste plek veroverd in de communicatie en zijn een factor geworden om rekening mee te houden. Ze zijn in staat reputaties te vestigen en reputaties te breken.

In dit hoofdstuk worden onder sociale media alle interactieve digitale toepassingen verstaan die gebruikers in staat stellen persoonlijke profielen te maken, te reageren op elkaars berichten, informatie te delen, contacten te onderhouden met andere gebruikers en eenvoudigweg exposure te vergroten.

Hoewel de voordelen van sociale media legio zijn, kleven er toch een aantal belangrijke risico's aan het gebruik ervan. In dit hoofdstuk wordt ingegaan op de risico's van sociale media, de voordelen van het gebruik ervan en uiteindelijk het vinden van een balans die veilig en verantwoord gebruik van sociale media mogelijk maakt.

Risico's in de praktijk

In september 2012 besloot een 15-jarig meisje de uitnodigingen voor haar verjaardagsfeest via Facebook te versturen. Op deze manier konden ze eenvoudig en op een snelle manier al haar vrienden bereiken. Het scheelde een hoop papierwerk, postzegels en het zoeken van de juiste adressen van haar vrienden. Nadat ze de uitnodiging geschreven had kon ze kiezen of dit aangemaakte evenement alleen voor genodigden is, voor alle contacten in haar vriendenlijst of dat het een openbaar evenement is. Ze vergat een keuze te maken, waardoor het evenement openbaar was en iedereen met een Facebook account de uitnodiging kon zien en aanmelden. De gevolgen zijn bekend. Geïnspireerd door de onder jongeren mateloos populaire film Project X verspreide de uitnodiging zich razendsnel door Nederland en trokken enkele duizenden jongeren naar Haren, het dorp waar de jarige woonde. Dit leidde tot flinke rellen, totaal verraste autoriteiten en een miljoenenschade voor de gemeente Haren.

Het illustreert het feit dat sociale media een ideaal platform kunnen vormen voor kwaadwillenden. Sociale media hebben namelijk een groot aantal gebruikers. Hierdoor kunnen kwaadwillenden de kracht van de massa aanwenden voor negatieve zaken, zoals men ook bij Project X Haren zag.

Daarnaast is ook (te) veel persoonlijke informatie via sociale media beschikbaar. Men moet er immers rekening mee houden dat alles dat op internet gezet wordt, nooit meer zal weg gaan en tot in de eeuwigheid beschikbaar kan blijven.
De jarige in de Haren casus had ook haar volledige adresgegevens gepubliceerd, waardoor iedereen die de beschikking heeft over een smartphone met één druk op de knop kon navigeren naar het huis van de jarige.

Het verzamelen van dit soort adresgegevens en andere persoonlijk informatie noemt men 'data mining'. Criminelen proberen zoveel mogelijk persoonlijke informatie te ontfutselen aan mensen, om vervolgens hun identiteit te kunnen overnemen.
Een persoon biedt bijvoorbeeld concertkaartjes te koop aan via Facebook of Twitter. Hij geeft aan dat hij vanwege een andere afspraak helaas niet het concert kan bezoeken en doet de kaartjes daarom voor een schappelijk prijsje van de hand. Hij geeft aan de anonimiteit van internet niet zo te vertrouwen en vraagt u daarom een kopie van uw legitimatiebewijs. Hij heeft dit ook nodig om de namen op de kaartjes te kunnen wijzigen bij de organisatie. Op het moment dat de kopie van het identiteitsbewijs binnen is, kan de crimineel via internet een bankrekening openen bij iedere Nederlandse bank op de naam van degene op het identiteitsbewijs. Binnen enkele minuten maakt hij duizenden euro buit. Tot voor kort dekten banken dergelijke verliezen, maar wanneer u de kleine lettertjes leest ziet u dat banken dit helemaal niet verplicht zijn.

De mondiale crisis trekt diepe sporen en ook in Nederland verliezen veel mensen hun baan. Gelukkig is er nu LinkedIn. Gedurende je carrière heb je een indrukwekkend netwerk opgebouwd en dat via LinkedIn gedigitaliseerd. Gelukkig komen er interessante vacatures voorbij. Een buitenlands bedrijf wil uw jarenlange ervaring graag gebruiken en vraagt u om enkele uren per week beschikbaar te zijn. Hun website ziet er goed uit en uit de persoonlijke berichten en gesprekken blijkt dat ze u graag willen hebben. U gaat in op het aanbod, ontvangt instructies en bedrijfsinformatie en u krijgt de beloofde bedrag voor het tekenen van het arbeidscontract. Op dat moment bent u een zogenaamde 'geldezel', een tussenpersoon die gebruikt wordt voor het doorsluizen van geld verdiend met criminele activiteiten. Dit is uiteraard strafbaar.

Een ander voorbeeld. U krijgt via sociale media een bericht dat er foto's van een vriend(in) van u op Facebook of Twitter staan, compleet met een link. Uit nieuwsgierigheid klikt u op de link om de foto's te

zien. Op dat moment wordt malware op uw computer of smartphone geïnstalleerd. Via deze malware kunnen criminelen meekijken en alle gegevens die u invoert kopiëren. De crimineel heeft nu uw bankgegevens en kan eenvoudig de rekening gaan plunderen.

Voordelen van gebruik

Toch wegen de nadelen van het gebruik van sociale media niet op tegen de vele voordelen. Zo is het bereik van sociale media groter dan vrijwel alle bekende advertentiemogelijkheden. Facebook heeft onlangs de grens van 1 miljard leden wereldwijd overschreden en kent in Nederland 8 miljoen leden. Ook Twitter is zeer populair in Nederland met 1,2 miljoen gebruikers. LinkedIn kan zich beroepen op 3,5 miljoen geregistreerde leden in dit land.

Zo bezien is exposure dus een van de grootste voordelen van sociale media. Organisaties kunnen op eenvoudige wijze hun doelgroep bereiken en hun boodschap overbrengen. Directe interactie met klanten of burgers is ook mogelijk en dat heeft veel bedrijven ertoe gebracht een zogenaamd 'web care' team op te richten dat zich bezighoudt met klachten of problemen van klanten. Zo kunnen bedrijven direct handelen wanneer er onvrede leeft onder de klanten of wanneer een geleverd product niet in orde is. Uit de praktijk blijkt dat zij sneller reageren wanneer een klacht wordt geuit via sociale media, dan op de reguliere manier via e-mail of telefoon. Wellicht omdat klachten zich als een veenbrand over sociale media kunnen verspreiden en veel mensen uw klacht kunnen zien. Bedrijven vrezen dan voor imago schade.

Ook voor de publieke sector biedt sociale media veel mogelijkheden. De politie maakt inmiddels veel gebruik van Twitter en vooral wijkagenten interacteren op deze wijze met de burgers in hun wijk, door begrip te kweken, waarschuwingen te kunnen uiten, zorgen van burgers te kunnen wegnemen en ondersteuning te krijgen bij het opsporen van verdachten. Dit heeft ook een afschrikkende werking.

Daarnaast is de snelheid van sociale media een belangrijk voordeel. Vanwege de miljoenen gebruikers is er altijd wel iemand met een sociale media account aanwezig bij belangrijke nieuwsgebeurtenissen. Tijdens de meteorieteninslag in Rusland onlangs, stonden de filmpjes van de inslagen al op het internet voordat de hulpdiensten waren uitgerukt. Een zelfde ontwikkeling ziet men bij conflicten. Burgers nemen alles op en delen het met de rest van de wereld, terwijl (buitenlandse) journalisten geen toegang krijgen tot de conflictgebieden, hun informatie uit indirecte bronnen moeten halen

en pas de volgende ochtend hun verhaal in de ochtendkrant kunnen plaatsen. Deze verhalen zijn dan vaak inmiddels weer ingehaald door de actualiteit en verliezen daardoor sterk aan nieuwswaarde. Daarbij spreken foto's en video's voor zich en zijn ze daarom vaak neutraler en minder politiek gekleurd dan reguliere media.

Sociale media zijn (vooralsnog) bijna allemaal kosteloos. Men kan zich gratis registreren op Facebook, Twitter, LinkedIn etc. en gebruik maken van vrijwel alle reguliere diensten. Dit stelt bedrijven in staat op zeer goedkope manier advertentiecampagnes te lanceren, gericht op een specifieke doelgroep.

Ook kan men eenvoudig profielen van mensen opstellen. Doordat voorkeuren en interesses openbaar weergegeven worden op sociale media, hebben ook bedrijven hier toegang toe. Op die manier kunnen zij advertenties nog beter toespitsen op specifieke personen. Wellicht hebt u zelf ooit een t-shirt gekocht via de webshop van bijvoorbeeld Wehkamp. U ziet dan vaak dat de advertenties in uw browser u ook verwijzen naar de nieuwste collectie shirts op de website van dit bedrijf.

Wanneer de campagne geen effect sorteert, dan kan deze meestal direct stopgezet worden zonder dat men vastzit aan een contract voor bepaalde tijd. Het beheer en onderhoud van de kanalen waarvan de campagne gebruik maakt is eenvoudig en laagdrempelig.

Verstandig gebruik

Zodoende is het zaak sociale media veilig te gebruiken. Ondanks dat de praktijk anders uitwijst, lijkt het overbodig om te stellen dat men bij iedere stap op sociale media dient na te denken over waarmee men bezig is. Ook is het belangrijk een aantal informatiebeveiligingsmaatregelen in acht te nemen.

Het spreekt wellicht vanzelf maar het is belangrijk niet te veel persoonlijke informatie op sociale media te delen. Immers het internet vergeet nooit en berichten zijn vaak tot in de eeuwigheid te vinden via bijvoorbeeld Google Cache. Kleine stukjes persoonlijke informatie op verschillende sociale media kunnen samengevoegd worden tot een profiel dat een behoorlijke indruk geeft van een bepaald persoon. Dit eerder besproken data mining is een nieuwe trend aan het worden onder criminelen.

Sommige mensen gebruiken ook hun camera voor sociale media activiteiten. Denk hierbij aan video chatten via Facebook of de

razendsnel in populariteit toenemende dating sites. Wanneer u naar de camera bovenin uw laptop of tablet kijkt, dan zult u vaak zien dat er geen schuifje voor zit. Hetzelfde geldt voor uw telefoon. Dit houdt in dat deze in principe altijd toegankelijk is. Kwaadwillenden kunnen ook dit hacken en van afstand door de camera van uw laptop meekijken. Zij kunnen hiermee opnames en foto's maken. Dit kan heel handig zijn voor bedrijfsspionage of om vast te stellen of de inventaris van uw huiskamer het waard is om een keer in te breken.

Toch is ook dit een risico dat makkelijk voorkomen kan worden. Als uw toestel een schuifje bevat, plaats het schuifje dan altijd voor de camera. Wanneer het schuifje ontbreekt, zoals in de meeste gevallen, kunt u er een stickertje opplakken.

Daarnaast is het verstandig te bedenken waar u gegevens achterlaat. Wanneer men bijvoorbeeld hetzelfde wachtwoord gebruikt voor verschillende sociale media en internetsites, dan dient men er ook rekening mee te houden dat dit wachtwoord bij een groot aantal mensen bekend is. Beheerders van een website kunnen immers in veel gevallen uw opgegeven wachtwoord ook inzien.
Wanneer bijvoorbeeld uw Hotmail of Gmail wachtwoord bekend is, dan kan een kwaadwillende eenvoudig alle wachtwoorden van uw sociale media accounts te pakken krijgen. Alle sociale media accounts zijn namelijk gekoppeld aan een e-mail adres dat u opgegeven heeft bij het aanmaken van de account. De crimineel (of woedende ex partner) hoeft dan slechts bij inloggen aan te geven dat hij/zij het wachtwoord vergeten is en een e-mail met link om het wachtwoord aan te passen wordt naar het e-mailadres gestuurd. De crimineel past de wachtwoorden aan en vervolgens heeft hij alle informatie in handen.

In 2012 werd LinkedIn gehackt en 6,5 miljoen wachtwoorden werd gepost op een Russisch forum voor hackers. Deze accounts werden vervolgens ontoegankelijk voor de eigenaren en alle informatie lag op straat. Omgedraaid loopt men dus ook een risico. Wanneer het wachtwoord van een sociale media account bekend is en men gebruikt dezelfde wachtwoorden, dat heeft de hacker ook eenvoudig toegang tot uw e-mail accounts.

Daarom is het belangrijk verschillende wachtwoorden te gebruiken voor verschillende soorten systemen. Wanneer u steeds hetzelfde wachtwoord gebruikt en dit wachtwoord wordt gehackt of geraden, dan heeft de hacker toegang tot al uw sociale media, privé en zakelijke e-mail.

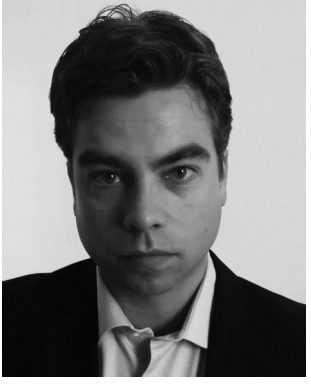
Het valt ook aan te raden een zogenaamd 'sterk' wachtwoord te gebruiken. Stel dat een wachtwoord van 8 karakters wordt gebruikt. Wanneer men alleen cijfers gebruikt, dan is dat wachtwoord met behulp van actuele software binnen 10 seconden te kraken zo blijkt uit onderzoek. Wanneer men letters, hoofdletters en cijfers gebruikt duurt dit ongeveer 250 dagen. Neemt men echter ook andere karakters, dan duurt dit bijna 57 jaar. Het is zodoende goed mogelijk een wachtwoord te kiezen dat niet eenvoudig gehackt kan worden.

Sociale media in balans

Men dient dus niet sociale media uit de weg te gaan. Voor veel individuele personen en bedrijven biedt sociale media een schat aan nieuwe kansen. Nog nooit was de afstand tussen multinationale bedrijven en de individuele consument dermate klein. De wereld ligt binnen handbereik en de mogelijkheden zijn eindeloos.

Het is alleen zeer belangrijk bij iedere stap die men zet op sociale media goed na te denken wat de consequenties kunnen zijn. Een eenvoudige manier is uw sociale media profiel te vergelijken met uw huis. Bedenk goed wat u niet opgeborgen achterlaat, wat in het zicht ligt en sluit ramen en deuren goed af. Laat geen vreemden binnen en accepteer alleen vrienden en kennissen. Wanneer u niet veel waardevolle spullen in huis heeft liggen, is het ook niet nodig de meest strenge beveiligingsmaatregelen te treffen. Maar zorg er wel voor dat er een fatsoenlijk slot op de deur zit en alleen u en uw gezinsleden een sleutel hebben.

U kunt er een prachtige woning van maken die helemaal aan uw wensen voldoet, maar hou niet voortdurend een open huizendag.



Raoul van Boekholdt werkt als security consultant voor Ordina. Zijn werkzaamheden hebben betrekking op privacy, awareness, sociale media en informatiebeveiliging.

Meer: www.ordina.nl