# Sociale netwerken zijn een must

Sociale media hebben een ingrijpende invloed gehad op de manier waarop wij met elkaar omgaan, communiceren, organiseren, onze meningen vormen, en zelfs winkelen. Deze media hebben grenzen doen vervagen, meer transparantie geboden en voor meer continuïteit gezorgd in alles wat we doen. Inmiddels is ongeveer tien procent van de gehele wereld met elkaar verbonden middels sociale media, en dat aandeel groeit dagelijks. Organisaties en bedrijven kunnen ze niet meer negeren of blokkeren. Sociale media maken deel uit van de wereld waarin we leven, leren, spelen en werken.

De realiteit is dat je dáár moet zijn waar je doelgroep zit, en die mensen vind je waarschijnlijk vaker terug op een sociaal medium dan op welk ander platform of locatie. Zowel klanten als partners en medewerkers verwachten met jou in contact te kunnen komen via sociale media. Het is voor jou als ondernemer dus een manier om in contact te blijven, feedback te verzamelen, medewerkers te werven en samen te werken. Daarom moet je sociale media in je omgeving ondersteunen om de innovatie mogelijk te maken, de productiviteit te verhogen en de groei te bevorderen die nodig is om je onderneming te laten overleven.

### Risico's van sociale media

Alles wat de sociale media zo aantrekkelijk maakt voor de gebruikers – het persoonlijke, het gemak waarmee informatie kan worden gedeeld, en de real-time aard van het medium – vormen aanzienlijke risico's voor je onderneming. Hieronder volgen de vier belangrijkste risico's waarmee je wordt geconfronteerd bij het gebruik van sociale media.

**1. Malware:** In 2010 werden de sociale media de favoriete communicatie-methode van de gebruikers. Deze gebruikers brengen meer dan 700 miljard minuten door alleen

al op Facebook, en daarmee maken zij sociale netwerksites en hun gebruikers tot ideale slachtoffers van malware. Uit een onderzoek van IT-beveiliger Sophos bleek dat 40% van alle gebruikers met malware geïnfecteerd was die afkomstig was van sociale netwerksites. De aanvallen van die malware maken gebruik van de vertrouwensband die is opgebouwd tussen de gebruikers en hun relaties. Zij (de malware-verspreiders) proberen gebruikers ertoe over te halen, informatie prijs te geven waarmee ze financieel voordeel kunnen behalen. Enkele voorbeelden van malware die met name succesvol is bij sociale media zijn:

- *phishing:* gebruikmakend van steeds slimmere technieken doen aanvallers zich voor als één van je legitieme sociale-netwerkrelaties en proberen je gevoelige informatie te ontlokken, zoals je inlogcodes. Ze maken misbruik van het feit dat veel mensen gewoonlijk voor al hun accounts dezelfde wachtwoorden gebruiken, en hopen dat als ze jou een gebruikersnaam en wachtwoord kunnen ontfutselen, ze toegang kunnen krijgen tot meer winstgevende accounts zoals je bankrekening en andere financiële en online accounts. De meeste gebruikers zijn er wel op bedacht om hun inlogcodes behorende bij hun financiële accounts niet prijs te geven, maar hun dagelijkse inlogcode tot een sociale netwerksite is slechts een kleine hindernis voor cybercriminelen om online zaken te stelen. Daarom richten steeds meer phishing-aanvallen zich op schijnbaar onbelangrijke online gebruikersaccounts.
- *click-jacking:* aanvallers proberen je te verleiden om op een link te klikken, bijvoorbeeld wordt zo'n link op je wall gepost en worden je vrienden gespamd met lokkertjes als 'kijk snel' of 'bekijk de foto's'. Als iemand dan op zo'n link klikt, installeren ze zonder dat ze het beseffen malware (code of script) die kan worden gebruikt om informatie te stelen of het beheer van de computer over te nemen. Clickjacking maakt misbruik van de dynamische aard van de sociale netwerksites en de bereidheid om te klikken op links op pagina's van mensen die je kent, en zelfs van mensen die je niet kent, om snel een groot publiek te bereiken. Zo verleiden ze je op slinkse wijze om privé-informatie prijs te geven (bijvoorbeeld door enquêtes), hits binnen te halen voor reclame-inkomsten, en uiteindelijk toegang te verkrijgen tot je gehele sociale netwerk.

**2. Verlies van gegevens:** Bij sociale netwerken gaat het om het opbouwen van relaties en het delen van ervaringen en informatie. Maar soms is het niet de bedoeling dat die informatie publiek gemaakt wordt. Het komt vrij vaak voor dat mensen argeloos vertrouwelijke informatie posten ('hé, ik heb zojuist een gesprek gehad met xxx en ik zie een forse commissie aankomen' of: 'ik ben radeloos, als we niet snel deze software-bug onschadelijk maken, heb ik een maand lang slapeloze nachten'). Dit kan geklassificeerd worden als 'interne kennis'. Er zijn ook gevallen bekend waarbij medewerkers onbewust op maat ontwikkelde software-codes op sociale netwerksites postten, en daarmee gevoelig intellectueel eigendom prijsgaven. Deze handelingen, hoewel niet doelbewust verricht, kunnen branche-specifieke verordeningen schenden, je reputatie aantasten, of je op achterstand zetten tegenover de concurrentie.

**'Om de organisatie te beschermen tegen gegevensverlies en te voldoen aan branche-specifieke verordeningen, moet je in staat zijn de handelingen te beheren die jouw medewerkers kunnen verrichten op de diverse sociale netwerksites'**

**3. Verbruik van bandbreedte:** Niet minder dan 40% van alle medewerkers geeft toe dat ze op hun werkplek op sociale netwerksites actief zijn. Met die activiteiten vormen ze een zware belasting van de beschikbare bandbreedte, wat ten koste gaat van andere zakelijke applicaties. Vorig jaar, toen de Amerikaanse regering open toegang toestond tot sociale netwerken, nam het verkeer over het internet toe met 25%. Alleen al video (denk aan alle filmpjes die je deelt met je vrienden en die je ophaalt van Facebook of Twitter) kan menig netwerk overbelasten. Een enkele video-stream verbruikt gewoonlijk tussen 500k en 1,2 Mbps (en dan hebben we het nog niet eens over HD, wat tussen de 4 en 7 Mbps opslorpt), en als tientallen of zelfs honderden mensen tegelijkertijd video's bekijken, is het logisch dat de algehele prestaties achteruit gaan.

**4. Productiviteitsverlies:** Sociale netwerksites worden online bestemmingen waar je boodschappen kunt posten en lezen, afspraakjes kunt maken, kunt winkelen, video's kunt up- of downloaden, en kunt gamen. Dat maakt ze in toenemende mate gemakkelijk en aantrekkelijk voor gebruikers, en verleidt hen om steeds meer tijd op die sites door te brengen. Van de andere kant vormen ze een

steeds grotere uitdaging voor de organisatie om het gebruik ervan in te tomen. Als er geen beperking op wordt aangebracht, kan de tijd die de medewerkers doorbrengen op de sociale netwerksites de productiviteit nadelig beïnvloeden. Ze spelen dan liever online games dan dat ze werken.

### Vereisten

Hoewel je beseft dat je het gebruik van de sociale media wel moet toestaan om te blijven concurreren en te kunnen groeien in de mondiale economie van vandaag, hoef je je onderneming nou ook weer niet bloot te stellen aan onnodige risico's. Er zijn manieren om je te beschermen tegen de risico's (of ze in ieder geval een stuk minder gevaarlijk te maken) die het sociale netwerken biedt. Je oplossing moet met name bevatten:

- een real-time web verdediging: het sociale netwerken verandert constant, en de tactieken die aanvallers gebruiken om er misbruik van te maken, veranderen mee. Als gevolg daarvan moet jouw oplossing het internetverkeer als het ware 'rennend' analyseren om bedreigingen te identificeren die zich daarop zouden kunnen bevinden. Real-time analyse van dynamisch veranderende links levert een acute risico-waarschuwing op waardoor tijdig beschermende maatregelen kunnen worden getroffen om de sociale media veilig te houden. Dus als je een melding krijgt als 'hé, kijk hier eens naar!', kun je daar ofwel op ingaan, dan wel dit wegklikken, afhankelijk van het potentiële risico dat dit oplevert.
- selectief sociale netwerk beheer: om de organisatie te beschermen tegen gegevensverlies en te voldoen aan branche-specifieke verordeningen, moet je in staat zijn de handelingen te beheren die jouw medewerkers kunnen verrichten op de diverse sociale netwerksites. Zo kun je bijvoorbeeld willen verhinderen dat medewerkers bijlagen, foto's of video's uploaden naar sociale netwerksites. Daarmee voorkom je risico's of ongewenst gegevensverlies en reputatieschade. Het gaat erom dat je tot in detail controle hebt over wat de medewerkers op de sociale media kunnen doen. Dit vereist een oplossing die niet alleen kijkt waar het initiële verkeer vandaan komt (bijvoorbeeld Facebook, YouTube, enzovoort) maar ook monitort wat er binnen die applicatie wordt gedaan (e-mail, het posten van boodschappen, het downloaden van bijlagen).
- caching: je kunt niet toestaan dat de sociale media je netwerk overbelasten en de werking van zakelijke applicaties nadelig beïnvloeden. Maar omdat sociale netwerken steeds meer een integraal onderdeel gaan uitmaken van de zakelijke processen, kun je ze niet zomaar blokkeren. Wat je wel kunt doen is elke potentiële degradatie van de prestaties ondervangen met caching. Daarmee kun je lokaal gegevens en videobestanden opslaan na een initiële download, en deze beschikbaar maken voor gebruikers die deze dan willen inzien. Op deze manier kun je de toegang tot sociale netwerken gewoon toestaan zonder dat de prestaties van ander verkeer op het netwerk daardoor worden aangetast.
- flexibel beleid: om de productiviteit te beheren, moet je in staat zijn een acceptabel gebruiksbeleid te hanteren voor wat betreft de sociale media. Je kunt er bijvoorbeeld voor kiezen om de toegang tot online games tijdens kantooruren te blokkeren; maar je kunt het ook toestaan en het een lagere prioriteit op het netwerk te geven zodat het geen nadelige invloed heeft op de zakelijke applicaties. Met een flexibel beleid kun je de activiteiten die je wel of niet toestaat, een prioriteit geven en tijden bepalen wanneer toegang wel toegestaan is. De mogelijkheid om te onderscheiden tussen sociale netwerksites en specifieke applicaties of content binnen die sites is van cruciaal belang voor het formuleren van een acceptabel gebruiksbeleid. Dus als je ervoor kiest om games te blokkeren, kun je zowel standalone games als games binnen sociale media-sites blokkeren. ■


**Auteur: Pierre Buijsman,**
Senior System Engineer bij Blue Coat (www.bluecoat.com)