

**business***bytes*



# Information Security anno 2011

## Trends, gevaren en oplossingen

---

dossier



<b>Inleiding</b> .....	<b>03</b>
Hoe veilig zijn de nieuwe manieren van werken?	

## *Trends*

<b>Solomo, de cloud en het Internet of Things</b> .....	<b>04</b>
Christophe Huygens, K.U.Leuven: 'Alles wordt met alles verbonden'	

## *Gevaren*

<b>Internetveiligheid in België</b> .....	<b>08</b>
Christian Van Heurck, CERT.be: 'We moeten ons securitymodel volledig herdenken'	

## *Oplossingen*

<b>Risicobeheer in de praktijk</b> .....	<b>11</b>
Xavier Mertens, Principal Security Consultant bij Telenet: 'Managers en eindgebruikers zijn cruciale schakels'	

<b>Woordenlijst</b> .....	<b>14</b>
---------------------------	-----------



# *Hoe veilig zijn de nieuwe manieren van werken?*

---

Werknemers beantwoorden thuis bedrijfsmails en lezen op het werk wel eens een Facebook-update. Ze nemen hun privét toestel mee naar kantoor en delen bestanden in de cloud. Deze nieuwe manieren van werken maken ondernemingen competitiever, maar de bedrijfsdata dreigen kwetsbaarder te worden, nu ze niet meer in een gesloten systeem zitten. Ondernemingen met een veelvoud aan persoonlijke, ongecontroleerde toestellen lopen niet alleen het risico belangrijke data te verliezen, ook het risico op malware neemt toe.

Omdat heel wat managers – en soms ook IT-deskundigen – nog maar weinig met de veiligheidsimplicaties vertrouwd zijn, zet dit dossier de grote lijnen uiteen. U leert waar de uitdagingen zitten en aan welke punten uw bedrijf aandacht zou moeten schenken. Ook zetten we u op weg naar oplossingen die gebruikscomfort, productiviteit en veiligheid met mekaar verzoenen.



# *“Alles wordt met alles verbonden”*

---

Christophe Huygens, security consultant en professor aan de K.U.Leuven





Een van de nieuw buzzwords in de technologiesector is solomo. Het acroniem staat voor de opmars en het samengaan van sociale, lokale en mobiele media. Voor Christophe Huygens, veiligheidsspecialist en professor aan het department Computerwetenschappen van de K.U.Leuven, is het een van de twee fenomenen die op korte termijn voor de beveiliging van data en netwerken van belang zijn. Het andere is cloud computing. Op langere termijn ziet hij vooral in de opmars van het Internet of Things (IoT) en machine-to-machinecommunicatie (M2M) een uitdaging voor veiligheidsspecialisten.

# Solomo, de cloud en het Internet of Things

---

‘De belangrijkste trend is ongetwijfeld dat de veiligheidsperimeter van het bedrijf niet meer bestaat’, zegt Huygens. ‘Door de opkomst van persoonlijke toestellen zoals de smartphone is het niet meer mogelijk om een onderneming hermetisch af te sluiten. Vooral met de nieuwe mobiele apparaten zitten bedrijven nu in een onveilige zone. Bedrijven moeten dat aanpakken, door hun beleid aan te passen en op de toestellen zelf maatregelen te nemen. Maar vooral de applicaties vormen een probleem. Bij Apple valt dat mee, omdat hun app store voor de iPhone een redelijk veilige walled garden is. Er wordt nog gecontroleerd wat daar in komt. Bij Android is dat niet het geval. Daar is eigenlijk alles mogelijk. Dat voedt de discussie die nu aan de gang

is over een kill switch, het op afstand wissen van gevaarlijke apps op een toestel. Europese overheden springen daar behoedzaam mee om, en vanuit het standpunt van de bescherming van de consument volg ik ze. Maar binnen een bedrijfscontext denk ik dat het wel moet kunnen. In elk geval moeten bedrijven een Acceptable Use Policy opstellen, zodat werknemers weten wat kan en wat niet kan. Ze moeten apps certificeren voor download, zodat werknemers weten met welke ze op het bedrijfsnetwerk kunnen, en met welke niet.’

## **Sociale media: niet voor kritische toepassingen**

De ‘mo’ in solomo is vanuit veiligheidsperspectief de belangrijkste bekommernis. Op het vlak van





- lokale en sociale toepassingen ziet Huygens minder problemen. De beveiliging van sociale media noemt hij wel 'heel zwak', maar het probleem is niet technisch. 'Met Twitter en Facebook zijn bijna wekelijks incidenten. Je zou die nochtans veel beter kunnen beveiligen. Maar het gebrek aan beveiliging heeft veel met marketing te maken, met het remmend effect van veiligheidsmaatregelen op het aantal gebruikers. Vermits de waarde van een sociaal netwerk stijgt met het aantal gebruikers, bouwen netwerk-sites liever niet te veel security in. Zolang het gebruik van sociale media onschuldig blijft, is dat nog aanvaardbaar. Als bedrijven sociale media enkel als marketingkanaal gebruiken, en niet voor kritische

toepassingen zoals het verspreiden van software-upgrades, zie ik geen al te grote problemen.'

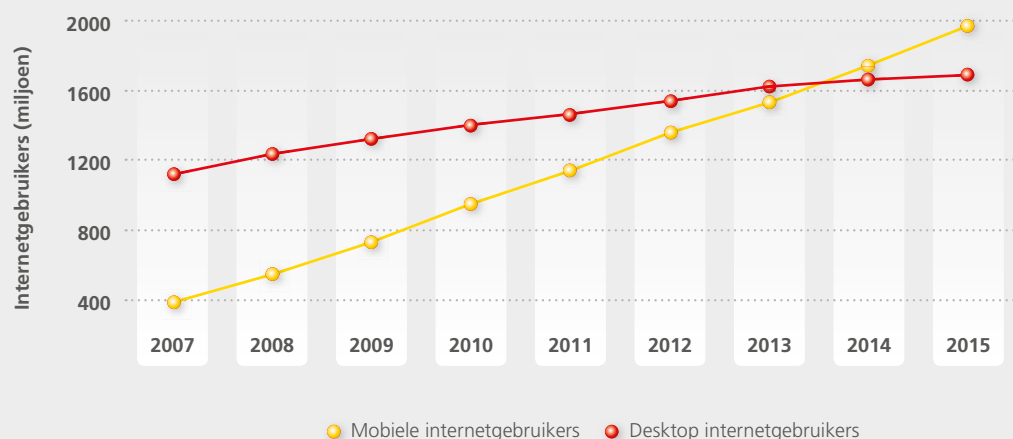
### Veiligheid in de wolk

Ook cloud computing kan voor Huygens gerust, want technisch kan cloud computing volledig veilig verlopen. Wel denkt Huygens dat veel mensen de impact ervan verkeerd inschatten. 'Als je aan cloud computing doet, wordt je internetconnectie veel belangrijker. Je hebt meerdere aansluitingen nodig en een hogere betrouwbaarheid. Wat risico betreft, krijg je dus heel andere aandachtspunten. Natuurlijk moet je alles encrypteren, maar je mag ook niet vergeten je processen en procedures aan te passen. ►►

## Mobiele groei

De groei van mobiele devices is zo sterk dat het Amerikaanse Morgan Stanley verwacht dat binnen enkele jaren het aantal mobiele internetgebruikers groter zal zijn dan het aantal desktopgebruikers. Door deze ontwikkeling verschuift ook de aandacht van criminelen en moeten veiligheidsspecialisten zich meer op mobiele beveiliging concentreren.

## Evolutie van het internetgebruik





## Managed services

Volgens professor Huygens zijn er heel wat oplossingen waarmee bedrijven hun netwerken en toestellen adequaat kunnen beveiligen. Maar het zijn deeloplossingen die nog geïntegreerd moeten worden, en daarvoor heb je expertise en consulting nodig. 'Security is zodanig specifiek dat alleen heel grote bedrijven de juiste kennis in huis kunnen halen en houden. Voor de meeste ondernemingen zijn managed services een veel betere oplossing. Een trusted partner neemt dan de beveiliging op zich.'

- ▶▶ Zo had je back-up en recovery vroeger volledig zelf in de hand, met cloud computing niet meer. Ook een audit uitvoeren wordt een stuk moeilijker. En dan zijn er de juridische implicaties. Als je data in een ander land staan, wat betekent dit dan? De wetgeving in Luxemburg is niet dezelfde als in Ierland. Vooraleer je aan cloud computing begint, moeten die vragen een antwoord krijgen.'

## Internet of Things

Op langere termijn komt er nog een volledig nieuwe uitdaging aan: het Internet of Things. Voorwerpen, machines en locaties worden via het internet verbonden, waardoor deze onderling of met mensen informatie kunnen uitwisselen. De trend is nu al ingezet. Christophe Huygens: 'Alles wordt met alles verbonden, wat het gemiddeld aantal apparaten per persoon spectaculair zal

doen stijgen. Voorzichtige ramingen spreken over duizend toestellen per persoon tegen 2015-2020. In de logistiek gaan we bijvoorbeeld elk pakje kunnen uitrusten met een actieve tag, zodat we het perfect kunnen volgen. In een bejaardentehuis gaan mensen een toestelletje krijgen, waardoor we ze snel kunnen terugvinden. En op een akker zal men duizenden apparaatjes samen met het zaaigoed uitstrooien, zodat de teelt beter gevolgd kan worden. Deze evolutie roept totaal nieuwe veiligheidsvragen op. Hoe gaan we bijvoorbeeld vertrouwen tussen toestellen in een netwerk op een dynamische manier tot stand brengen? Hoe gaan we bepaalde handelingen van machines controleren? Daarvoor gaan we gedragsanalyse van apparaten nodig hebben en kleine applicatiespecifieke en policygedreven firewalls. Hier wordt nu al volop aan gewerkt, ook in ons onderzoekscentrum.' ■



**Christophe Huygens** is security consultant en professor aan de K.U.Leuven. Hij stond mee aan de wieg van NetVision/Ubizen en is vandaag verbonden aan de IBBT-onderzoeksgroep DistriNet, die zich specialiseert in gedistribueerde computersystemen en beveiliging. Aan de K.U.Leuven doceert Huygens momenteel computernetwerken en computer- en netwerkbeveiliging.



# *We moeten ons security- model volledig herdenken*

---

Christian Van Heurck, veiligheidsanalist en coördinator van CERT.be





In de media verschijnen regelmatig berichten over cybercriminaliteit. Maar hoe groot zijn de gevaren werkelijk, en hoe pakken we ze aan? CERT.be, het Belgische Computer Emergency Response Team verzamelt informatie over de risico's en bedreigingen in ons land.

# Internetveiligheid in België

Voor Christian Van Heurck, coördinator ad interim, is de 'romantische' tijd van de individuele hacker die vanuit zijn zolderkamertje een groot bedrijf trachtte binnen te dringen duidelijk voorbij. Vandaag komen de gevaren vooral vanuit de hoek van de georganiseerde misdaad. De beveiliging van een bedrijf kraken is big business geworden. Gestolen kredietkaarten of patiëntendossiers worden vlot verhandeld op de zwarte markt. Malware is zelfs een Software as a Service (SaaS) geworden, die je

inclusief garanties kunt huren. Als voorbeeld van de schaal waarop vandaag criminelen handelen, verwijst Van Heurck naar het Rustock-botnet, dat dagelijks miljarden spammails verspreidde vanaf naar schatting één miljoen geïnfecteerde computers. 'Dit soort botnets wordt groter en krachtiger. Het wordt steeds moeilijker om ze tegen te houden, want ze hebben een eigen anti-anti-virus aan boord en ze gebruiken steeds gesofisticeerdere encryptie en communicatietechnieken.'



## Meldpunt voor veiligheidsproblemen

CERT.be is het nationale meldpunt voor internetbedreigingen en -kwetsbaarheden. CERT.be werkt samen met gelijkaardige organisaties in het buitenland. Christian Van Heurck: 'We werken op basis van vertrouwen met mekaar, in een gesloten groep van mensen die elkaar persoonlijk kent. Informatie-uitwisseling gebeurt via restricted mailinglists of persoonlijk contact en altijd zonder de gegevens over betrokken bedrijven te vermelden. Wij spreken onderling enkel over IP-adressen.'

### Veiligheidsincidenten melden

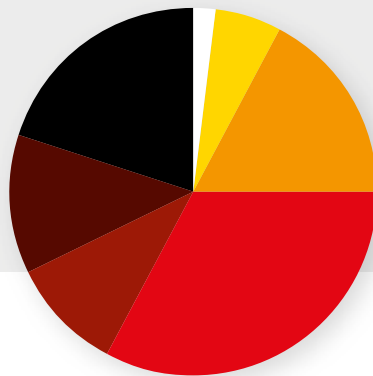
- Via CERT.be
- Per e-mail: [cert@cert.be](mailto:cert@cert.be)

Een geëncrypteerde mail sturen, bellen of faxen kan ook.

**Meer gegevens hierover vindt u op [www.cert.be](http://www.cert.be)**



### Soorten incidenten, eerste helft 2011



● Accountdiefstal.....	2%
● Denial of service attacks.....	6%
● Spam.....	17%
● Gehackte systemen.....	33%
● Wormen en virussen.....	10%
● Scans.....	12%
● Andere.....	20%

#### ►► Geen magische oplossingen

In de huidige context kan beveiliging niet meer van één product komen, beklemtoont Van Heurck. 'Managers in bedrijven denken soms dat alles met één product op te lossen valt. Of kleine KMO's, dat een recent anti-virusprogramma volstaat. Dit is vandaag echt onvoldoende om van een veilige omgeving te kunnen spreken. Door de BYOD-trend (Bring Your Own Device) moeten we ons securitymodel volledig herdenken.'

'Die trend heeft de perimeter van het bedrijf doen verdwijnen, waardoor nu alles in principe untrusted is. Je kan daar moeilijk tegenin gaan en alles gaan afsluiten en verbieden. Een al te strikte beveiliging kan de gebruiksvriendelijkheid in de weg staan. En dan gaan mensen een omweg zoeken, waardoor je de onveiligheid onrechtstreeks zelfs in de hand werkt.' Volgens Van Heurck zijn er geen magische oplossingen, wel een veelvoud aan deeloplossingen.

'En vergelijk het met huizen en auto's: men breekt eerst in waar dat het makkelijkst gaat.'

#### Brandweer

Concreet advies over beveiligingsoplossingen geeft CERT.be niet. Van Heurck: 'We zijn in de eerste plaats een neutraal meldpunt. Bedrijven die een veiligheidsprobleem hebben, kunnen dat bij ons in alle vertrouwen melden. Je moet ons zien als de brandweer, niet de politie. Bij de politie moet je aangifte doen. Mensen weten niet altijd hoe dat moet; ze hebben toelating van het hoogste management nodig; en ze vrezen soms voor imagoschade. Bij ons zijn al die drempels er niet. Wij houden alles vertrouwelijk. Als bedrijven ons problemen melden, krijgen we een beter zicht op het groter geheel en kunnen we effectiever helpen. Als meerdere partijen dezelfde problemen ondervinden, kunnen we bijvoorbeeld makkelijker en sneller de gemeenschappelijke oorsprong ervan achterhalen.' ■



**Christian Van Heurck** is veiligheidsanalist en coördinator van CERT.be. Hij werkte voordien als systeem- en applicatiemanager bij CultuurNet Vlaanderen en als IT-manager bij Telepolis.



# *“Managers & eindgebruikers zijn cruciale schakels”*

---

Xavier Mertens, Principal Security Consultant bij Telenet





‘Veiligheid is veel meer dan een technische oplossing’, zegt Xavier Mertens, security consultant bij Telenet. Voor een goede beveiliging is het van groot belang dat bedrijfsmanagers en beveiligingsspecialisten elkaar begrijpen, en dat eindgebruikers zich bewust zijn van de hele veiligheidsproblematiek. ‘Technisch is er veel mogelijk, maar managers en eindgebruikers moeten ook mee zijn.’

# Risicobeheer in de praktijk

Xavier Mertens: ‘Een manager die geen of weinig veiligheidsincidenten heeft meegemaakt, zal naar de kostprijs van beveiliging kijken en zich –begrijpelijk– afvragen of het allemaal wel nodig is. Een systeem voor logbeheer, dat je toelaat te zien wat er allemaal op je netwerk gebeurt, is vanuit veiligheidsstandpunt bijvoorbeeld onontbeerlijk. Je kan met zo’n systeem volgen wat er gebeurt en wie erbij betrokken is. Het kost natuurlijk geld, en dan zie je dat sommige managers terughoudend reageren. Maar je moet zo’n systeem zien als een verzekering. De kans dat je huis afbrandt, is relatief

klein. Toch betaalt iedereen een verzekeringspremie om zich te beschermen tegen het risico. Zo is het ook met de beveiliging van data en netwerken. Eén incident kan een grote impact hebben op de werking van je onderneming en op je bedrijfs-  
imago. Daartegen moet je je beschermen met een adequate beveiliging.’

### **Bewustzijn**

Ook eindgebruikers zien het nut van beveiliging niet altijd. Ze ruilen gebruiksgemak of functionaliteiten liever niet in voor meer veiligheid. Voor ►►

### **Telenets architectuurbenadering**

De beveiligingsaanpak van Telenet is gebaseerd op een grondige architectuurbenadering. Op basis van een analyse van de bestaande infrastructuur en de behoeften van de klant worden de meest geschikte componenten geselecteerd en geïmplementeerd.

**Meer informatie op [www.telenet.be/security/opmaat](http://www.telenet.be/security/opmaat)**



## Beveiligingspakketten voor kleinere organisaties

Telenet brengt enkele nieuwe next generation internet security solutions op de markt waarmee kleine bedrijven hun internetconnectie beter kunnen beveiligen. U kunt met deze oplossingen bepaalde internetapplicaties blokkeren (bijvoorbeeld Facebook) zonder de volledige verbinding af te sluiten. Het gaat om managed solutions die Telenet zelf installeert en beheert, er is geen kennis en geen hardware-investering vereist.

[www.telenet.be/security/pakketten](http://www.telenet.be/security/pakketten)

- ▶▶ Xavier Mertens vormen ze de zwakste schakel in de veiligheidsketen. 'Ten eerste loop je altijd het risico dat er in je organisatie gebruikers met slechte bedoelingen rondlopen. Of mensen die kwaadwillig de beveiliging doorbreken, bijvoorbeeld omdat ze net ontslagen zijn. Het is belangrijk dat je daar als bedrijf goed mee omgaat en bij ontslag bijvoorbeeld onmiddellijk alle toegang tot de infrastructuur blokkeert. Maar daar zitten eigenlijk niet de grootste risico's, want het gaat om een zeer kleine groep. Je hebt een veel groter aantal mensen dat volledig ter goeder trouw is, maar toch de veiligheid in het gedrang brengt. Mensen die 's avonds nog wat willen doorwerken en daarom bijvoorbeeld bedrijfsgegevens op een stick mee naar huis nemen. Dat zijn goede medewerkers met veel motivatie, maar wat als zo'n onbeveiligde stick onderweg verloren raakt of gestolen wordt? Wat als de gegevens thuis op een onbeveiligde computer worden gezet? Bewustmakingsprogramma's zijn heel belangrijk om werknemers op dit soort problemen attent te ma-

ken. Soms zie je ook dat mensen onveilig handelen omdat ze anders gewoonweg niet kunnen werken. Mensen geven bijvoorbeeld hun wachtwoord door omdat een collega anders niet verder kan. In zulke gevallen moet je het systeem natuurlijk aanpassen.'

### Samenwerking

'Om tot een oplossing te komen die zowel voor managers als eindgebruikers voldoet, is veel communicatie nodig', zegt Xavier Mertens. 'Uiteindelijk komt beveiliging altijd in samenspraak tot stand. Als partner moeten we rekening houden met de budgettaire bekommernissen van managers, inzicht verwerven in de infrastructuur en in de processen van het bedrijf. Pas dan gaan we kijken naar specifieke veiligheidstoepassingen die we kunnen invoeren. En als we dan samen voor een bepaalde beveiliging kiezen, moeten we onze keuzes ook aan alle werknemers in een verstaanbare taal kunnen uitleggen. Onze taak als veiligheidsspecialist gaat dus veel verder dan het technische.' ■



**Xavier Mertens** is Principal Security Consultant bij Telenet. Hij noemt beveiliging 'een passie' en heeft zich de afgelopen jaren gespecialiseerd in security monitoring, rapportering en auditing. Net als de andere veiligheidsspecialisten van Telenet schoolt hij zich permanent bij. Xavier heeft zo tal van internationaal erkende veiligheidscertificaten verworven.



# Woordenlijst

---

## **Acceptable Use Policy (AUP)**

Een beleidsdocument dat de regels omvat waaraan werknemers zich op een bedrijfsnetwerk dienen te houden. Een AUP omschrijft toegelaten en ongeoorloofd gebruik. Medewerkers krijgen netwerktoegang na ondertekening van het document.

## **Botnet**

Een netwerk van besmette computers die door een centraal commandopunt aangestuurd worden om criminele activiteiten uit te voeren. Een geïnfecteerde computer maakt deel uit van een botnet zonder dat de eigenaar zich daar bewust van is.

## **Bring Your Own Device (BYOD)**

BYOD is een businessmodel dat werknemers toelaat een persoonlijk toestel (laptop, smartphone, tablet) te gebruiken op het werk. BYOD wordt ingevoerd omdat het kostenefficiënt is voor de werkgever en werknemers mobieler en productiever maakt. Het vraagt wel om een specifieke beveiligingsaanpak.

## **Cloud computing**

Het gedeeld gebruik van servers, applicaties en andere resources op afstand, via eenvoudige, gebruiksvriendelijke netwerktoegang.

## **Denial of service (DOS) attack**

Een groot aantal besmette computers maakt, aangestuurd door een centraal commandopunt, gelijktijdig een verbinding met een server waardoor deze tijdelijk niet meer beschikbaar is of crasht.

## **Internet of Things (IoT)**

De verbinding van voorwerpen, machines en locaties via het internet, waardoor deze onderling of met mensen informatie kunnen uitwisselen.

## **Malware**

Verzamelnaam voor kwaadaardige software, zoals virussen, wormen, botnets en spyware.

## **Social engineering**

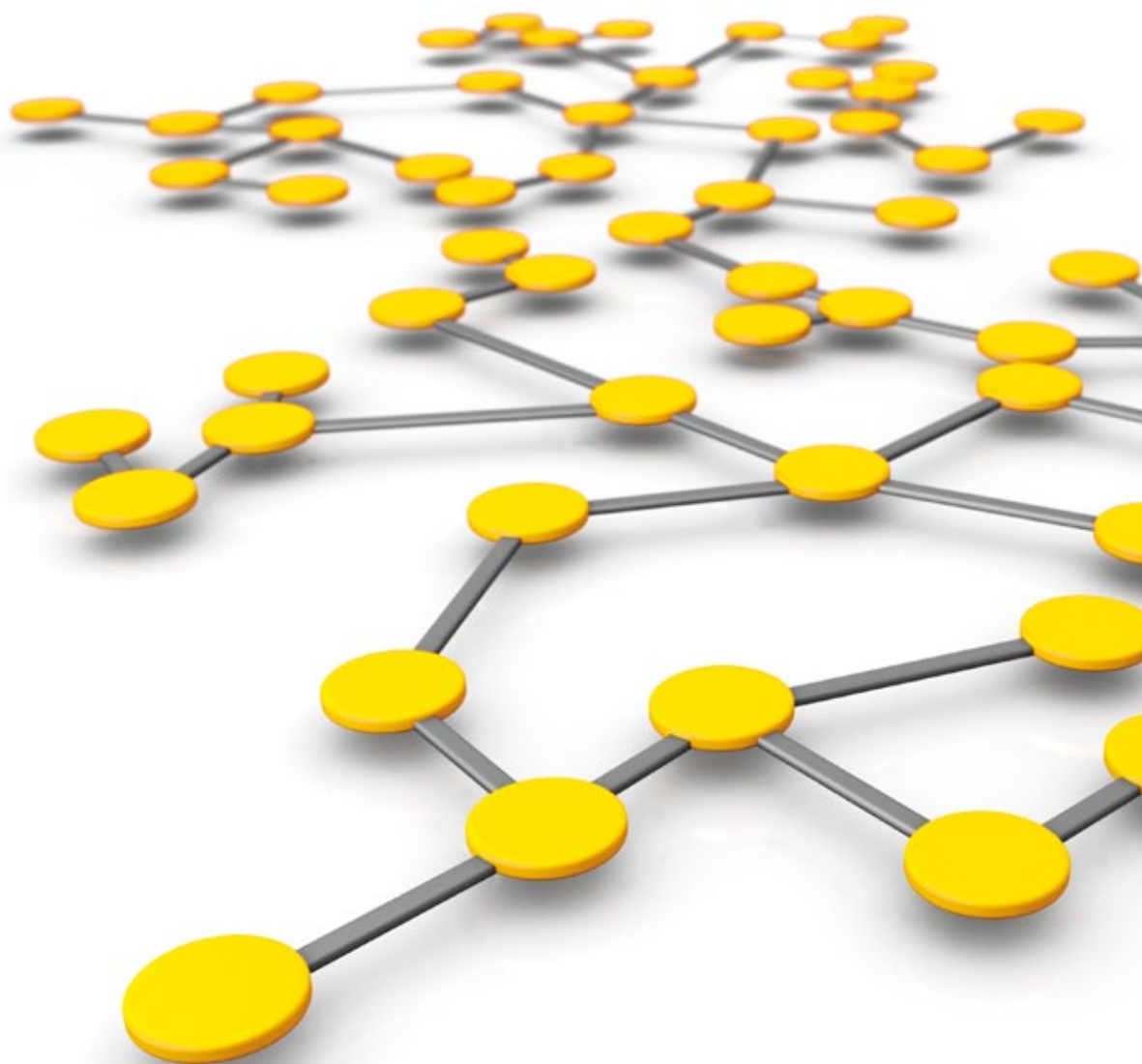
Het stelen van vertrouwelijke of geheime informatie door misleiding van computergebruikers. E-mails die de ontvanger vragen om kredietkaartnummers of wachtwoorden door te mailen, zijn vormen van social engineering. Ook phishing-websites (getrouwe kopieën van echte websites), die nietsvermoedende bezoekers doen inloggen met vertrouwelijke gegevens, zijn een voorbeeld.

## **Solomo**

De opmars en het samengaan van sociale, lokale en mobiele media. Nieuwe term, gelanceerd tijdens een evenement bij Google, begin 2011.

## **Walled garden**

Een gecontroleerde omgeving van applicaties en bestanden. Downloaden vanuit een walled garden biedt meer garanties op het vlak van de veiligheid.



## Security Competence Center

Telenet wil bedrijven helpen om niet alleen productiever, maar ook veiliger te werken. Daarom heeft het een eigen Security Competence Center (SCC) opgericht. In het SCC werken ongeveer 35 veiligheidsspecialisten die ondernemingen adviseren omtrent de beveiliging van hun netwerk en data.

[www.telenet.be/security](http://www.telenet.be/security) | 015 36 47 47

