Digital Confidence

Sleutel tot de digitale groei van morgen

LIBERTYGLOBAL
POLICY SERIES

booz&co.

Digital Confidence

Sleutel tot de digitale groei van morgen

Vertaald uit het Engels

DIGITAL CONFIDENCE: DE KERNPUNTEN

• Naar verwachting zal de digitale economie in Europa met 18 procent per jaar groeien tot 2012; van €236 miljard in 2008 tot €436 miljard in 2012.

• Tot voor kort werd de groei in de digitale economie voor een belangrijk deel bepaald door de uitbreiding van infrastructuren en technologische ontwikkelingen, zoals digitale tv (DTV) en breedbandtechnologieën van de volgende generatie.

• De komende tijd zal sprake zijn van een zeer aanzienlijke waardeverschuiving van toegang – nog steeds winstgevend en op beperkte schaal groeiend – richting elektronische handel, online- en digitale content-aanbiedingen en online adverteren.

• Toenemend gebruik en toenemende uitgaven per gebruiker zullen de komende vijf jaar zorgen voor meer groei: met name bedrijven in content en reclame zullen sterk groeien. E-commerce blijft de grootste markt in absolute zin.

• Desondanks gaan deze groeifactoren te maken krijgen met sterke krachten in de Europese informatie-maatschappij. Zoals Web 2.0-diensten die zich over platforms uitbreiden (online, DTV, mobiel) en een nieuwe, "born digital" generatie consumenten die volledig "connected" zijn, overal aan meedoen, maar ook zeer assertief zijn; dit leidt tot veel aandacht van pers en politiek.

• Door de groei en het succes van de digitale wereld maken veel consumenten en ondernemingen zich zorgen over de veiligheid en integriteit van de digitale omgeving.

• Het verbeteren van de Digital Confidence, als maatstaf voor het vertrouwen van consumenten en leveranciers in digitale en onlinediensten, is dan ook in hoge mate bepalend voor de groei van de digitale economie – of staat het juist in de weg. Een marktvolume van €124 miljard (2012) kan op het spel staan, ongeveer 1 procent van het BBP (bruto binnenlands product) voor de EU-27. Content en reclame lopen hierbij het grootste risico. De economische winst als het lukt om vertrouwen te doen toenemen loopt op tot 11 procent extra groei (of €46 miljard), boven op de €436 miljard "base case". Mocht het niet lukken om Digital Confidence te verbeteren, dan wordt het verlies groter: 18 procent (of €78 miljard) kan verloren gaan.

• Alle spelers in de sector zijn het erover eens dat hun reputatie inzake Digital Confidence opgebouwd moet worden en hebben daartoe een brede reeks activiteiten geïnitieerd. Toch is er tot op heden een duidelijk gebrek aan coherentie en gemeenschappelijke focus; de meeste acties zijn ad hoc, naar aanleiding van veelbesproken incidenten waarbij sprake was van vertrouwens- of veiligheidsbreuken en politieke druk.

• Wetgeving alleen kan de snelheid en veelheid aan uitdagingen in deze markt niet bijhouden. Vandaar dat succesvolle bedrijven meer doen dan alleen de wetgeving naleven – zij blijven een slag voor door proactief beleidslijnen en handelswijzen aan te nemen die Digital Confidence versterken.

• Digital Confidence steunt op vier pijlers die samen de belangrijkste punten van zorg bij consumenten en bedrijven adresseren:

1. Netwerkintegriteit en Quality of Service (QoS).
Gericht op het voorzien in veilige en veerkrachtige technologieplatforms voor de digitale wereld en het leveren van optimale gebruikerservaring.
2. Privacy- en databescherming.
Richt zich op zorgen van individuen met betrekking tot hun digitale data.
3. Bescherming van minderjarigen.
Beoogt het welzijn van minderjarigen online te beschermen.
4. Preventie illegaal kopiëren en diefstal.
Beoogt een veilige digitale zakenomgeving te bieden voor alle belanghebbenden.

• Als beheerders van de klantrelatie moeten netwerkoperators beleidslijnen en methodes gebruiken die in brede zin aanvaard worden

door de gebruiker. Dit gaat verder dan het voldoen aan wettelijke vereisten of het dienen van de belangen van bepaalde belanghebbenden.

• Beleid en handelswijzen moeten dan ook niet bepaald worden door op zichzelf staande zaken (zoals illegaal kopiëren), maar getuigen van een holistische benadering van alle onderdelen van Digital Confidence, omdat de implicaties van dergelijke beleidslijnen in de praktijk samenvallen en tegenstrijdige reacties kunnen oproepen bij belanghebbenden.

• Belangrijke lessen uit casestudies wereldwijd laten zien dat een "can-do"-visie realistisch is: om Digital Confidence te verbeteren kunnen netwerkoperators meer zijn dan "doorgeefluik" en opvoeder/onderwijzer terwijl zij tegelijkertijd richtlijnen voor aanvaardbaar klantgedrag respecteren en wettelijke "veilige havens" met het oog op aansprakelijkheden beschermen.

• Gebaseerd op analyse van een aantal casestudies komen een aantal best practices met het oog op acceptatie door de consument bovendrijven:

  • Consumenten accepteren transparante, handelswijzen – netwerkoperators, serviceproviders, content- en platformspelers dienen dergelijke communicatie in samenwerking met de regelgever te stimuleren.

  • Consumenten zijn bezorgd over de manier waarop netwerkoperators en ISP's omgaan met hun digitale gegevens – duidelijke uitleg en een consistent en betrouwbaar regelgevend kader hebben hier de hoogste prioriteit.

  • Consumenten eisen eigen risicobeheer – dit vraagt om toegang tot de geschikte hulpmiddelen, opt-in-/opt-out mechanismen en voorlichting.

  • Consumenten accepteren maatregelen die Quality of Service garanderen – als dit actief dataverkeermanagement vereist, staan ze daar voor open, vooropgesteld dat voorwaarden duidelijk zijn.

• Om zeker te zijn van juist gedoseerde interventie en algemene gebruikersacceptatie, moeten netwerkoperators bij het hanteren van een proactiever beleid en methodes een gefaseerde aanpak volgen, gebaseerd op het E3-paradigma: Educate eerst, Empower vervolgens, Enforce waar nodig.

• Beleid en handelswijzen op het gebied van Digital Confidence moeten worden ingebed in de betrokken organisaties door interne protocollen en besluitvormingsstructuren te ontwikkelen. Deze zullen richting moeten geven aan toekomstige producten en diensten; aan keuze van en implementatie van netwerk technologieën en veiligheidsoplossingen; en aan de communicatie naar consumenten en andere belanghebbenden (bijvoorbeeld industriespelers, contenteigenaren, regelgevers).

I. SAMENVATTING

DE VOLGENDE GROEIFASE IN DE DIGITALE WERELD: GEBRUIK BEPAALT DE GROEI, NIET HET AANTAL GEBRUIKERS

Europa's digitale economie heeft een sterk groeiperspectief, gestimuleerd door web 2.0-services die inmiddels gemeengoed zijn geworden en gebruik maken van de functionaliteit, beschikbaarheid en toegenomen capaciteit van breedbandnetwerken. Migratie naar netwerken van de volgende generatie, een toenemende verscheidenheid aan inventieve netwerk-technologieën en de nieuwe generatie steeds meer assertieve "born digital" consumenten zijn krachten die het digitale economische ecosysteem onder grote druk zetten. Dit nieuwe paradigma vormt een grote uitdaging voor zowel de sector in het algemeen als voor de beleidsmakers en regelgevende instanties.

Er staan grote belangen op het spel: wij verwachten dat de Europese markt voor digitale diensten groeit naar €436 miljard in 2012, met een totale jaarlijkse groei van 18 procent (2007-2012).

Tot op heden wordt de groei in internetgebruik grotendeels bepaald door de opkomst van nieuwe technologieën (zoals breedband en DTV). Deze technologieën hebben veel markten op het gebied van internettoegang bijna geheel verzadigd. De nieuwe golf van digitale groei zal dan ook meer bepaald worden door toenemende inkomsten per individuele gebruiker, dan door het aantal gebruikers. Naar verwachting zal deze groei worden bereikt door meer innovatieve producten en diensten, aangevuld met nieuwe businessmodellen die meer opbrengsten genereren. De belangrijkste economische groeisectoren zijn, in volgorde van hun respectieve groei: reclame, content, e-commerce en toegang.

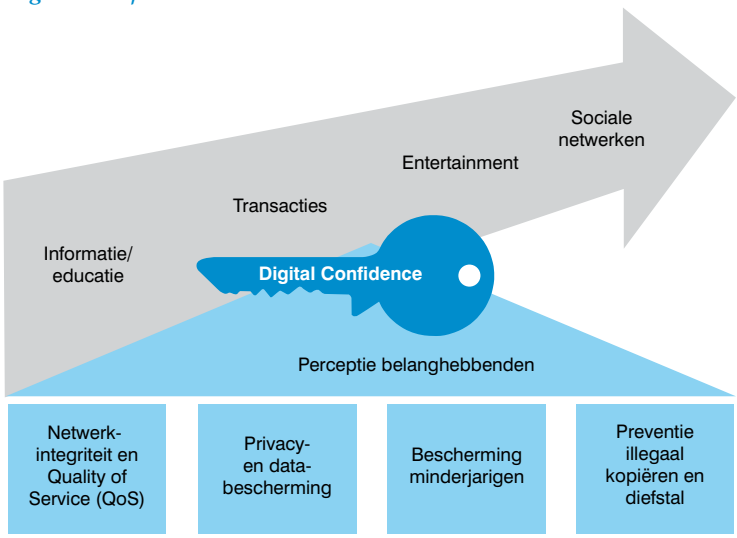
De groei en het succes van de digitale wereld brengen voor veel consumenten en ondernemingen zorgen met zich mee over de veiligheid en de integriteit van de digitale omgeving. De mate waarin consumenten vertrouwen hebben in dienstverleners en platformproviders, hun manier van zakendoen en de veiligheid van hun diensten en netwerkomgevingen, plus het vermogen van overheden en regelgevende instanties om veiligheidsnormen voor de consument te garanderen, is een belangrijke factor geworden voor de digitale economische groei.

Het is van groot belang om overeenstemming te bereiken met betrekking tot de prioriteiten op het gebied van verbetering van vertrouwen en veiligheid. De rollen en verantwoordelijkheden van alle spelers moeten worden gedefinieerd en men moet weten welke mogelijke hulpmiddelen en maatregelen kunnen worden toegepast. Dit rapport is bedoeld om een feitenbasis voor de discussie te verstrekken en om raamwerken, een gemeenschappelijke taal en ideeën te introduceren. Aan de hand hiervan kan overeenstemming bereikt worden en waar nodig een gezamenlijk – of gecoördineerd – beleid tot stand worden gebracht.

DIGITAL CONFIDENCE: SLEUTEL TOT DE DIGITALE GROEI VAN MORGEN

Tegen deze achtergrond wordt het verbeteren van vertrouwen en veiligheid een belangrijke drijfkracht voor de toekomstige groei van de digitale wereld. Dit is met name van belang omdat de "born digital" consumenten steeds assertiever worden en snel reageren door hun gebruik te verminderen of actie te voeren waar pers en politiek bij betrokken worden – vaak met inzet van web 2.0-technologieën. Op basis van interviews met 50 deskundigen uit heel Europa en de VS en een systematisch overzicht van marktgegevens alsmede best practices en perspectieven in de sector, hebben wij vier pijlers geïdentificeerd die de belangrijkste zorgen van consumenten

Digital Confidence raamwerk



en bedrijven met betrekking tot de huidige en toekomstige digitale wereld adresseren:

- **Netwerkintegriteit en Quality of Service** bij consumenten en bedrijven: beschermen van technologieplatforms tegen aanvallen van buitenaf en het zekerstellen van optimale internetverbindingen ongeacht piekuren of criminele aanvallen, alsook het beveiligen van de computeromgeving van zowel consumenten als bedrijven tegen storingen door virussen en andere malware.

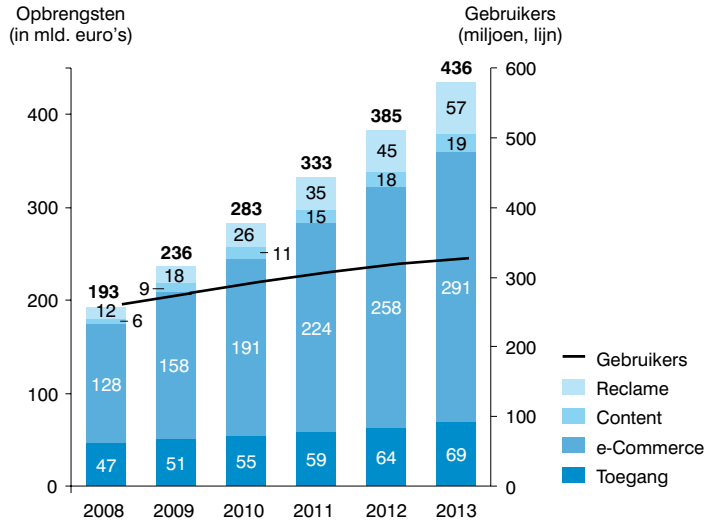
- **Privacy en databescherming**: verhinderen dat elektronische persoonsgegevens (identiteiten, wachtwoorden, gebruik- en consumptieprofielen, enz.) worden gebruikt, gepubliceerd of commercieel uitgebuit zonder toestemming en het verhinderen van identiteitsdiefstal en -fraude.

- **Bescherming van minderjarigen**: beschermen van kinderen tegen blootstelling aan ongewenste content, verhinderen van pesten en ander vijandig gedrag, voorkomen van grooming en andere vormen van uitlokking door volwassenen en de strijd tegen kinderpornografie.

- **Preventie van illegaal kopiëren en diefstal**: het tegengaan van diefstal van auteursrechtelijk beschermde content en het beschermen van e-commerce-transacties.

De sector moet proactief handelen vanuit een holistische visie. Een dergelijke benadering is gevat in het concept "Digital Confidence". Digital Confidence gaat verder dan het naleven van de wet – het is voor operators reeds een commerciële noodzaak en voorwaarde aan het worden. Zoals bepaalde voorbeelden zullen aantonen, betekent het naleven van de wet nog geen aanvaarding door de consument. Beleid en de bedrijfsvoering van operators dienen alle hieraan gerelateerde wettelijke, economische en maatschappelijke aspecten gezamenlijk aan te pakken om de volgende fase van de groei van de digitale wereld mogelijk te maken.

Europese online opbrengsten en gebruikers

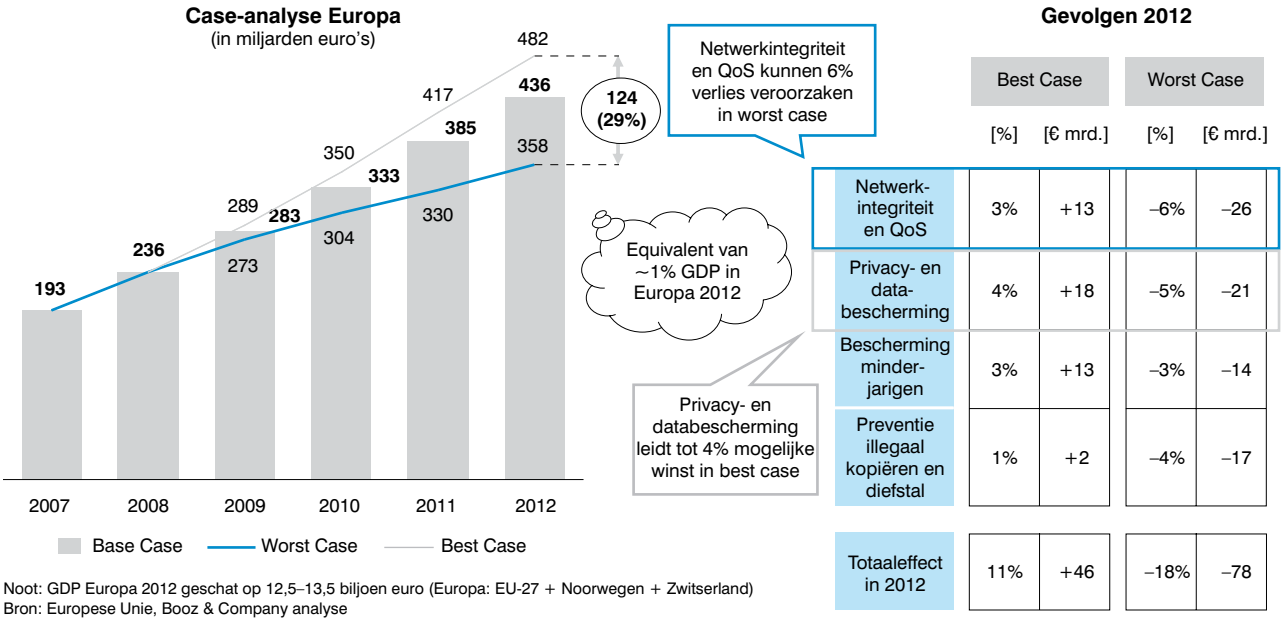


Noot: Europa inclusief EU-26, Noorwegen en Zwitserland
Bron: Forrester e-Commerce Forecast, Bedrijfsrapportage Apple, Bedrijfsrapportage Google, EU TV and Broadband Forecast Model, Booz & Company analyse

RISICO-/BATENANALYSE: DIGITAL CONFIDENCE LOONT

Volgens onderzoek en analyse van Booz & Company staat in Europa een markt van €436 miljard in digitale toegang, handel, content en reclame op het spel, met een totale jaarlijkse groei van 18 procent tegen 2012. Het verschil tussen een "geslaagde Digital Confidence aanpak" in het beste geval en een "mislukte Digital Confidence aanpak" in het slechtste, komt op €124 miljard, ofwel bijna 30 procent van de totale markt – ongeveer 1 procent van het totale EU-27+2 BBP in 2012! Het gecombineerde verlies bij het "mislukken" van Digital Confidence is met €78 miljard veel groter dan de winst van €46 miljard – hoofdzakelijk bepaald door de gevolgen van "Netwerkintegriteit en Quality of Service" en "Privacy- en databescherming" is financieel belangrijk, vooral, maar niet uitsluitend, door de implicaties ervan voor innovatieve bedrijfsmodellen in reclame (bijvoorbeeld gerichte reclame gebaseerd op surfgedrag). Consumenten zijn wellicht minder geneigd tot e-commerce, aankoop van digitale content of abonnementen op innovatieve digitale diensten als het vertrouwen ontbreekt in de manier waarop hun persoonlijke gegevens worden behandeld en beveiligd. "Netwerkintegriteit en Quality of Service" zijn onmisbaar om de voortdurende groei van content en videodiensten te ondersteunen. Indien goed beheerd zullen netwerken grote bandbreedte kunnen leveren voor een Quality of Service die de digitale wereld voor alle gebruikers ondersteunt. "Preventie illegaal kopiëren en diefstal" is van belang voor zowel content-eigenaren als e-Commerce. Naast de vanzelfsprekende inkomstenimplicaties van de contentsector door het beschermen van de waarde van hun rechtenportfolio's en de introductie van innovatieve digitale en online businessmodellen, bestaat er een aanzienlijk risico van een negatieve impact op e-commerce transacties als consumenten overstappen op offline kanalen, wat voor veel nieuwe businessmodellen (bijvoorbeeld online-veilingen) niet mogelijk is.
De inkomstencategorieën die het gevoeligst zijn

Invloed Digital Confidence



Gevolgen 2012

	Best Case		Worst Case	
	[%]	[€ mrd.]	[%]	[€ mrd.]
Netwerk-integriteit en QoS	3%	+13	–6%	–26
Privacy- en data-bescherming	4%	+18	–5%	–21
Bescherming minder-jarigen	3%	+13	–3%	–14
Preventie illegaal kopiëren en diefstal	1%	+2	–4%	–17
Totaaleffect in 2012	11%	+46	–18%	–78

Noot: GDP Europa 2012 geschat op 12,5–13,5 biljoen euro (Europa: EU-27 + Noorwegen + Zwitserland)
Bron: Europese Unie, Booz & Company analyse

voor Digital Confidence zijn content- en reclamemarkten. Beide markten zijn nog jong en hun ontwikkeling is sterk afhankelijk van Digital Confidence: reclame kan ernstig worden tegengewerkt door negatieve reacties van consumenten als het niet op een door gebruikers aanvaarde manier wordt geimplementeerd, of door te beperkende wetgeving. Het zeer beperkend beschermen van consumentenprivacy kan bijvoorbeeld van invloed zijn op nieuwe businessmodellen gebaseerd op gerichte en gepersonaliseerde reclame – reclame die een belangrijke bijdrage levert aan de Europese online-reclamemarkt van €57 miljard in 2012. Bovendien zal reclame een centrale rol spelen bij het financieren van alle opkomende en snelgroeiende Web 2.0-services, zoals sites voor sociaal netwerken en innovatieve contentaanbiedingen. Contentproviders vrezen dat excessief illegaal kopiëren hun digitale businessmodellen ernstig op de proef kan stellen. Het risico voor e-commerce is relatief kleiner, maar absoluut gezien door het businessvolume het grootst: het draagt €52 miljard bij aan het mogelijke verlies en de helft daarvan aan de mogelijke winst van Digital Confidence.

Zuiver economisch gezien en de bredere maatschappelijke aspecten even negerend, toont de risico/batenanalyse aan dat de digitale sector er aanzienlijk economisch voordeel bij heeft om alle gebieden van Digital Confidence samenhangend te benaderen, om in elk geval negatieve groeiscenario's te vermijden en te streven naar de best mogelijke groeiscenario's.
Alle spelers in de sector zijn het erover eens dat hun reputatie inzake Digital Confidence verder opgebouwd moet worden en hebben daartoe een brede reeks activiteiten geïnitieerd. Toch is er tot nog toe een duidelijk gebrek aan coherentie en gemeenschappelijke focus; de meeste acties zijn ad hoc, naar aanleiding van veelbesproken incidenten waarbij sprake was van een grote vertrouwens- of veiligheidsbreuk en politieke druk.

Het belangrijkste onderscheid tussen het beste en het slechtste scenario is de mate van eensgezindheid in de bedrijfstak over de aanpak van Digital Confidence. Eensgezindheid betekent niet noodzakelijkerwijs dat iedereen alles op dezelfde manier doet; het gaat eerder om de mate van overeenstemming in de bedrijfstak als geheel om de neuzen dezelfde kant op te zetten. Het gaat om de mate waarin er een gemeenschappelijk visie is betreffende algemene prioriteiten en daaruit voortkomende verantwoordelijkheden die dat voor iedere belanghebbende met zich meebrengt.

Netwerkproviders moeten een belangrijke rol blijven spelen omdat hun kernactiviteit de genoemde krachten achter de economische groei in belangrijke mate mogelijk maakt. Het niveau van integriteit van het netwerk heeft een grote economische invloed, zelfs al lijkt de kernactiviteit van een provider – toegang – het minst te zijn blootgesteld aan de baten en risico's van het al dan niet slagen van Digital Confidence.

FRAMEWORK FOR ACTION

De pijlers van Digital Confidence moeten alle vier dringend worden aangepakt. Ze zijn sterk

afhankelijk van elkaar en dragen alle bij aan het algemene beeld van een veilige, of onveilige, digitale wereld.

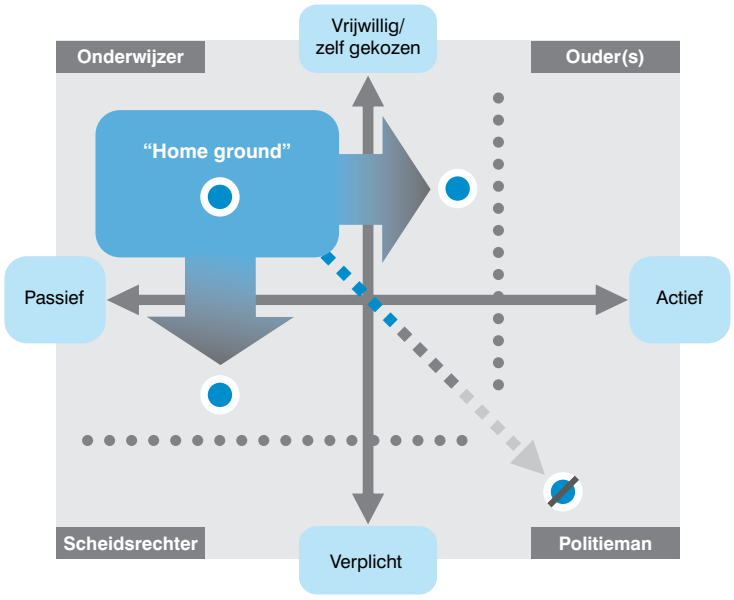
Door de complexiteit van de genoemde kwesties en de onderlinge afhankelijkheid van veel spelers in de gehele waardeketen wordt duidelijk dat iedereen een bepaalde rol heeft in de digitale economie. Hoewel netwerkoperators op veel gebieden oplossingen kunnen leveren, kunnen ze duidelijk slechts hun deel bijdragen aan de hele puzzel.

Om de diverse rollen die de netwerkoperators kunnen spelen op de genoemde probleemgebieden te laten zien, is een "Digital Confidence positioneringsmodel" ontwikkeld. Dit model beschrijft de manier waarop maatregelen worden getroffen (bijvoorbeeld passief, "hands-off", of actief met een "volledige controle"-aanpak) en onderscheidt de onderliggende principes. De daaruit voortvloeiende rollen kunnen worden gekoppeld aan algemene maatschappelijke functies. Bijvoorbeeld:

- De onderwijzer informeert gebruikers zoveel mogelijk over mogelijkheden en bedreigingen, maar zal doorgaans niet actief corrigerend optreden (voorbeeld: "Web Wise Kids" met informatief materiaal voor kinderen op het internet).

- De ouder informeert evenals de onderwijzer gebruikers over bedreigingen en maatregelen, maar treedt proactief op als gebruikers beschermd moeten worden (bijv. YouTube dat auteursrechtelijk beschermde filtert).

Positionering: de "Home Ground" van internet providers



- De scheidsrechter vertrouwt van geval tot geval eerder op zelfopgelegde handhaving van regels en richtlijnen dan op voorlichting, maar die regels zijn gebaseerd op wederzijdse instemming (bijv.: UPC NL dat proactief toegang beperkt tot internetdomeinen met seksueel kindermisbruik).

- De politieagent is van nature geneigd wetgeving strikt uit te voeren, alle noodzakelijke maatregelen te nemen en doet dat op basis van strikte regels, zoals alle onwettige activiteiten blokkeren (bijv. implementatie van een "three strikes you're out" regel bij schending van auteursrechten).

Bij het bepalen van hun positie moeten de netwerkoperators echter heel zorgvuldig zijn in hun rol zodra die valt buiten hun primaire bedrijfsactiviteit en verantwoordelijkheid. Elke maatregel die hun wettelijke veilige haven als "doorgeefluik" kan ondermijnen en hen kan blootstellen aan onbeheersbare aansprakelijkheden, zal uiteindelijk niet bijdragen aan het verbeteren van Digital Confidence – terwijl het publiek daar juist hooggespannen verwachtingen van zou hebben gekregen.

Op basis van onze analyse van successen en mislukkingen op het gebied van Digital Confidence lijkt er een traditionele "thuisbasis" te bestaan voor netwerkoperators: een positie die "onderwijzer" wordt genoemd – gericht op het zoveel mogelijk inlichten van gebruikers over mogelijkheden en bedreigingen – maar die normaal gesproken niet proactief optreedt. Op grond van deze "thuisbasis" zou dan alleen nog aan wetgeving hoeven voldoen te worden. Onze analyse laat echter duidelijk zien dat dit in de toekomst niet genoeg zal zijn.

Wetgeving kan vaak de snelheid van en veelheid aan veranderingen met betrekking tot Digital Confidence niet bijhouden. Netwerkoperators zijn eigenaar van de klantrelaties en moeten beleidslijnen en praktijken toepassen die door de gebruiker worden aanvaard en dat gaat verder dan het naleven van wettelijke vereisten of het dienen van de belangen van bepaalde betrokkenen.

Succesvolle bedrijven doen dan ook meer dan alleen naleven: ze proberen een slag vóór te blijven door sommige belangrijke principes ter bevordering van Digital Confidence na te leven:

- Ze werken aan procedures en protocollen die vertrouwen scheppen.

• Ze zijn zo open en transparant mogelijk in hun communicatie met de consument.

• Ze spannen zich in om klanten goed te informeren en in staat te stellen hun belangen in de digitale wereld zelf te beschermen.

Om te zorgen voor een verhoudingsgewijze aanpak en om algemene aanvaarding van gebruikers te verkrijgen voor een meer proactief beleid en handelswijze, dienen netwerkoperators een gefaseerde benadering te volgen, gebaseerd op het E3-paradigma: Educate eerst, Empower vervolgens, Enforce waar nodig – met andere woorden, eerst informeren, dan zelfbescherming mogelijk maken en waar nodig bescherming opleggen.

Uit de geanalyseerde gevallen komen een aantal best practices met betrekking tot acceptatie door de consument naar voren:

• Consumenten accepteren transparante, niet-storende handelswijzen – netwerkoperators, serviceproviders, content- en platformspelers dienen dergelijke communicatie in samenwerking met de regelgever te stimuleren.

• Consumenten zijn bezorgd over de manier waarop netwerkoperators en ISP's omgaan met hun digitale gegevens – duidelijke uitleg en een consistent en betrouwbaar regelgevend kader hebben hier de hoogste prioriteit.

• Consumenten eisen eigen risicobeheer – dit vraagt om toegang tot de geschikte hulpmiddelen, opt-in-/opt-out mechanismen en voorlichting.

• Consumenten accepteren maatregelen die Quality of Service garanderen – als dit actief dataverkeermanagement vereist, staan ze daar voor open, vooropgesteld dat er duidelijke voorwaarden worden gecommuniceerd.

Deze principes gelden voor alle belanghebbenden.

Vervolgens moeten beleid en handelswijzen op het gebied van Digital Confidence worden ingebed in de betrokken organisaties. Met het oog op de implicaties voor netwerkoperators moeten de activiteiten op één lijn gebracht worden om prestaties op het gebied van Digital Confidence naar een hoger niveau te tillen. Providers moeten op vijf niveaus handelen:

1. BELEID EN PROCEDURES

Netwerkoperators en ISP's moeten hun positie ten aanzien van Digital Confidence duidelijk maken door hun strategie en positie ten aanzien van alle vier pijlers uiteen te zetten. Dit moet de basis vormen voor alle beleidslijnen inzake Digital Confidence. Deze positionering moet gedetailleerd genoeg zijn om concreet inzicht te geven in de onderliggende vragen over deze kwesties, bijvoorbeeld hoe een bedrijf de afweging maakt tussen ongepaste content en vrijheid van meningsuiting

Als volgende stap moet dit beleid ingebed worden in de kernactiviteiten van het bedrijf. In de meeste gevallen zal dit direct van invloed zijn op de manier waarop netwerkoperators denken over productontwikkeling, bijvoorbeeld door te zorgen dat alle producten en diensten voldoen aan hun eigen normen.

Daarnaast moeten netwerkoperators hun beleid en procedures voor Digital Confidence actueel houden door beide regelmatig te toetsen aan juridische aspecten, openbaar beleid en techniek.

Ten slotte verwijzen de in dit rapport geanalyseerde gevallen naar een belangrijke les: Digital Confidence vereist vertrouwen en de beste basis voor vertrouwen is open communicatie: transparantie loont. Bedrijven zouden dan ook open moeten zijn over hun beleid en de redenering erachter, ook zakelijk. De ervaring leert dat aanvaarding door de consument in het algemeen groot is als regels en de onderliggende redenering openlijk duidelijk worden gemaakt. Hierdoor ontstaat ook een dialoog met de consument, wat zeer nuttig kan zijn om oplossingen te verbeteren.

2. GOVERNANCE

Kwesties rond Digital Confidence zijn complex, zeer gevoelig en over en weer van invloed op elkaar. Vaak vereisen ze dat een bedrijf fundamentele posities inneemt, bijvoorbeeld hoe er wordt omgegaan met seksueel misbruik content. Een verkeerde beslissing betekent aanzienlijke risico's, zowel financieel als voor de goede naam van het bedrijf. Het is dan ook uitermate belangrijk om hier op top managementniveau aandacht aan te schenken. Digital Confidence moet ook duidelijk worden ingebed in de organisatiestructuur door bijvoorbeeld een Raad voor Digital Confidence te benoemen met voldoende senior toezicht en de autoriteit om alle gerelateerde activiteiten te overzien en te implementeren.

3. TECHNOLOGIE

De voor Digital Confidence vereiste technieken zijn op grote schaal voorhanden, nu richt

de aandacht zich vooral op het beslissen over individuele positionering, het vaststellen van geschikt beleid en het creëren van ondersteunende beleidsstructuren. Toch moet de meerderheid van de netwerkoperators nog investeren in bepaalde technologieën, ter voorbereiding op de toekomst. Het gaat er daarbij bijvoorbeeld om de Quality of Service te handhaven gezien de toenemende (diversiteit in) multimediaverkeer. Netwerkoperators zullen hierover moeten beslissen door een evenwicht te vinden tussen het toevoegen van transportcapaciteit en actief dataverkeermanagement, middels gefaseerde tarieven of technische maatregelen. Verder dienen ze samen te werken met contentproviders om hun netwerken te optimaliseren voor het doorgeven van multimediacontent, zoals peer-to-peer caches (bijvoorbeeld de aanpak ontwikkeld door het P4P-initiatief) of netwerken die content leveren. Regelgevers zullen willen weten dat het probleem op de juiste manier wordt aangepakt.

Een ander groot technologisch risico vormt de apparatuur van de eindgebruiker. Die is in de meeste gevallen niet voldoende beveiligd tegen bedreigingen als virussen, botnets en andere malware. Softwareoplossingen bestaan al wel, maar netwerkoperators en ISP's moeten hun klanten nog actiever aanmoedigen die ook te gebruiken. Netwerkoperators en ISP's moeten bovendien hulpmiddelen en oplossingen inzetten die de consumenten in staat stellen zelf controle te houden over het risico dat ze lopen. Dit kan bijvoorbeeld middels een opt-in-/opt-out keuzemogelijkheid. Dat vereist wel dat er meer actie wordt ondernomen. Het aanbieden van oplossingen die van de website gedownload kunnen worden is niet voldoende; netwerkoperators en ISP's moeten met programma's komen die het aantal geïnstalleerde oplossingen stimuleren en controleren.

4. CONSUMENTENVOORLICHTING

Netwerkoperators en ISP's moeten zich samen met NGO's richten op, en tevens zelf initiatieven nemen voor, geschikte voorlichting (bijvoorbeeld informatiecampagnes op hun eigen websites).

Deze voorlichtingsprogramma's moeten zien op bedreigingen op het gebied van publicatie van persoonsgegevens, gerichte reclame, illegaal kopiëren en ongewenst online gedrag in het algemeen (waaronder ook pesten, uitlokking en onaanvaardbare content).

Voorlichting moet gericht plaatsvinden, afgestemd op specifieke gebruikersgroepen, inclusief ouders en kinderen. Het programma voor de ouders moet zich richten op het monitoren van de activiteiten van kinderen en hen bewust maken van de bedreigingen op het internet – en de hulpmiddelen laten zien die hen ter beschikking staan om de online-omgeving van hun kinderen te beheren. Voorlichting voor kinderen dient zich te richten op het herkennen van – en omgaan met bedreigingen.

5. REGULERING

Netwerkoperators moeten regelgevers aansporen tot specifieke acties ter ondersteuning van de inspanningen om proactief vertrouwen op te bouwen op gebieden waar netwerkoperators of ISP's geen invloed hebben (bijvoorbeeld zwarte lijsten van illegale content, wetshandhaving). Regelgevers moeten ervoor waken om niet te proactief regels op te stellen, tenzij ze er zeker van zijn dat de maatregelen proportioneel zijn.

Op haar beurt moet de bedrijfstak duidelijk laten zien dat ze Digital Confidence serieus neemt door de ontwikkeling van coherente oplossingen te initiëren. Bij dergelijke oplossingen moeten alle spelers betrokken zijn en de implementatiekosten en latere opbrengsten dienen evenredig te worden verdeeld. Regelgevers moeten de bedrijfstak de ruimte geven om dergelijke oplossingen te ontwikkelen en zowel medewerking van de belanghebbenden als financiële steunprogramma's stimuleren. Daarbij moeten ze de concurrentie in het voordeel van de consument laten werken, in plaats van regelgeving toe te passen die, hoe goed bedoeld ook, contraproductief kan zijn vanuit het oogpunt van de consument en economische schade kan veroorzaken. Onze analyse toont bijvoorbeeld aan dat strikte Quality of Service-regelgeving die de meeste vormen van dataverkeermanagement verbiedt, de investeringsbehoeften van netwerkoperators in heel Europa tot €6 miljard kan doen toenemen.

Bij het uitvoeren van maatregelen in al deze vijf initiatiefgebieden wordt netwerkoperators en ISP's aangeraden zoveel mogelijk samen te werken met NGO's. Veel aspecten kunnen effectiever worden aangepakt als een operator samen met een NGO het initiatief neemt; de NGO kan neutraliteit en sectorbrede inzetbaarheid waarborgen, gebruikmakend van de goede reputatie van NGO's. Recent onderzoek wijst uit dat consumenten veel vertrouwen hebben in NGO's.

PRIORITEITEN VOOR REGELGEVERS

Regelgevers en overheidsinstanties moeten hun positie bepalen op dit gebied, dat zich beweegt tussen censuur en consumentenvoorlichting, strenge regelgeving en zelfregulerende vrijemarktfilosofieën. Door de grensoverschrijdende aard van de bedreigingen voor Digital

Confidence is er nadrukkelijk behoefte aan met name internationale (juridische) samenwerking. Dit om het bewustzijn van de noodzaak tot handelen te vergroten en, voor overheden en wetshandhavers, om geschikte middelen toe te wijzen voor effectieve handelingsstructuren en partnerships met de bedrijfstak. Tot op heden werkt het gebrek aan een coherente benadering uiteindelijk in het nadeel van de consumenten: transparantie en informatie over de risico's en voordelen van de digitale wereld ontbreken, terwijl ondernemingen staan voor de uitdaging duurzame, nieuwe digitale businessmodellen te ontwikkelen.

Het ziet ernaar uit dat de politiek en regelgevende instanties meer nadruk leggen op medewerking van belanghebbenden en co-regulering in plaats van het ontwikkelen van meer wetgeving. Tegelijkertijd zal er behoefte zijn aan voortdurend onderzoek naar de juiste dosering van elke vorm van regelgeving, zeker als het een zeer interventionistische aanpak betreft (zoals het "three strikes you're out" of het opleggen van verplichte netwerkfilters) die wellicht een inbreuk vormen op elementaire internetvrijheden en fundamentele consumentenrechten (bijvoorbeeld privacy) en verworven juridische zekerheden van de bedrijfstak ondermijnen.

Regelgevers hebben ongetwijfeld een belangrijke rol in het zekerstellen van Digital Confidence. Gezien de complexiteit van Digital Confidence kunnen regelgevers bijvoorbeeld meer samenwerking met de belanghebbenden bevorderen. De volgende gebieden verdienen de voortdurende aandacht van de regelgevers:

• Stimuleer netwerkoperators en ISP's om beleid en procedures inzake Digital Confidence vast te stellen; en stimuleer zelfregulering op basis van gedragsregels voor de bedrijfstak – met name waar dwingendere regelgevende interventie kan leiden tot negatieve economische resultaten (bijvoorbeeld in dataverkeermanagement), of fundamentele consumentenrechten kan schenden (bijvoorbeeld de "Three strikes"-regel).

• Overweeg maatregelen om het juridische - en eventueel het reputatierisico te beperken voor netwerkoperators en ISP's die beleid en procedures voor Digital Confidence introduceren. Neem bijvoorbeeld de leiding in het ontwikkelen van een register van internetsites die verwijderd en verboden zijn in het belang van de bescherming van minderjarigen en stimuleer het gebruik ervan. Breng in Europa eenheid aan in de op dit moment per land zo verschillende aanpak in deze; zorg daarbij voor constructies die het mogelijk maken op internationaal niveau de bescherming van minderjarigen te coördineren.

• Creëer stimuleringsmaatregelen om de bedrijfstak een meer actieve rol te laten spelen bij het informeren van consumenten – zorg voor financiering en neem overkoepelende initiatieven om grootschaliger te kunnen werken, door bijvoorbeeld voort te bouwen op de resultaten van het Safer Internet Programme.

• Doe meer aan internationale samenwerking om wereldwijde (raamwerken voor) oplossingen te ontwikkelingen voor deze feitelijk wereldwijde problemen, bijvoorbeeld op het gebied van copyrightbescherming.

• Besteed vooral aandacht aan de onderlinge afhankelijkheid van de verschillende gebieden van Digital Confidence voor de diverse belanghebbenden en stem beslissingen hierop af. Zo kan handhaving van zeer strikte regels wat betreft Quality of Service onbedoelde consequenties hebben, zoals aanzienlijke kosten voor netwerkupgrades die uiteindelijk de kosten voor de consument verhogen.

Samengevat hoeft Digital Confidence niet veel te kosten – in benodigde investeringen – om te slagen. Aan de andere kant zouden de kosten van mislukking aanzienlijk zijn. Een programma om Digital Confidence te laten slagen is evenwel niet gemakkelijk en ook niet gratis. De meeste CEO's zijn van mening dat hun organisaties al bezig zijn met de bovenomschreven activiteiten, en terecht. Maar in de meeste gevallen is dat niet genoeg. Digital Confidence reikt verder dan het ter beschikking stellen van voorlichtingsmateriaal op de website. Het gaat erom op topniveau de toonaangevende instanties op dit gebied, privaat of publiek, erbij te betrekken en serieuze campagnes te lanceren die daadwerkelijk een verschil maken. Hier is geld voor nodig en wellicht ook nieuwe vaardigheden binnen de organisaties. Digital Confidence gaat niet alleen over het hebben van een beleid voor dataprivacy; het gaat erom als bedrijf een andere denkwijze te ontwikkelen, een andere manier van communiceren met klanten en de bredere gemeenschap. Kortom, Digital Confidence vereist leiderschap vanaf de top.

II. DE VOLGENDE GROEIFASE IN DE DIGITALE WERELD: GEBRUIK BEPAALT DE GROEI, NIET HET AANTAL GEBRUIKERS

1. DE DIGITALE WERELD: INLEIDING

Digitale technologieën hebben het dagelijks leven – thuis en op het werk – in een adembenemend tempo veranderd. Kortere ontwikkelingscycli en als gevolg daarvan steeds sterkere apparatuur hebben, in combinatie met de drastisch kortere vervangingscycli van technologieën thuis, geleid tot een massamarkt penetratie van digitale technologie. Of het nu contact maken en communiceren met vrienden, films kijken, naar muziek luisteren of foto's nemen betreft – de wereld is digitaal. Digitale technologieën zijn allang niet meer het domein van technologiefreaks en hebben een centrale plaats in het moderne leven. De meeste consumenten vinden het vandaag de dag erger om hun internetverbinding thuis te verliezen dan hun telefoonaansluiting.

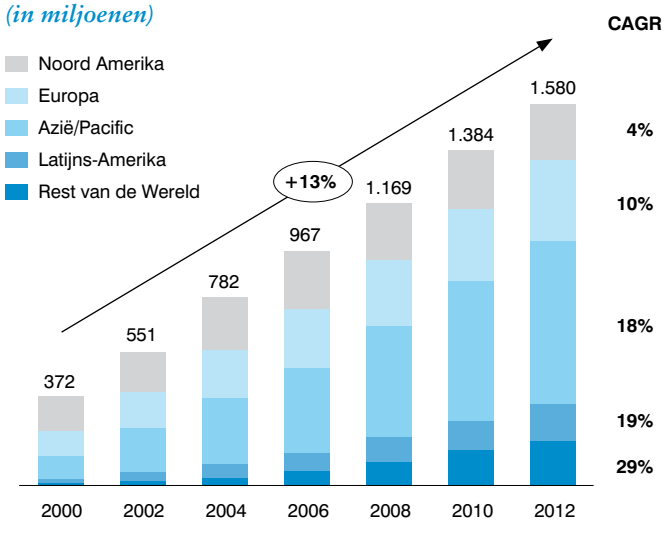
Uit de recentste ontwikkeling van digitale diensten, van digitale tv tot zogenaamde Web 2.0-toepassingen, blijkt het onmiskenbaar duidelijk: het volledige potentieel van digitale technologie en diensten komt pas goed tot zijn recht als technologieën en toepassingen een fysiek en logisch netwerk vormen. Wat is de echte revolutie in digitale fotografie: het feit dat celluloid filmrolletjes van de plank verdwenen of dat de beelden binnen enkele minuten met vrienden kunnen worden gedeeld? Vooral Web 2.0-toepassingen zoals Facebook en YouTube die zich richten op de sociale aspecten van digitale technologie, onderstrepen dit. Als de communicatie, de samenleving, de content en de commercie worden gecombineerd is de toegevoegde waarde voor de consument enorm – en in veel gevallen uiterst innovatief. De explosieve groeicijfers van deze diensten in alle westerse economieën en daarbuiten vormen hiervan een indrukwekkend bewijs. Interessant genoeg profiteren al deze diensten direct zelf van dat sociale aspect: viral marketing, dat wil zeggen mond-tot-mond- of pc-tot-pc-communicatie, is de belangrijkste drijfkracht achter hun groei. Dit alles is alleen mogelijk in een genetwerkte omgeving.

In deze context is een belangrijk gegeven dat de meerderheid van de Europese huishoudens (binnenkort) is voorzien van drie digitale netwerkverbindingen: internet, digitale tv en mobiel. Stuk voor stuk in verschillende mate in staat om breedbanddiensten te leveren en alle – ook in verschillende mate – interactief.

De internetnet- en breedbandpenetratie hebben bijna het verzadigingspunt bereikt: in veel Europese landen is de penetratie hoger dan 70 procent.

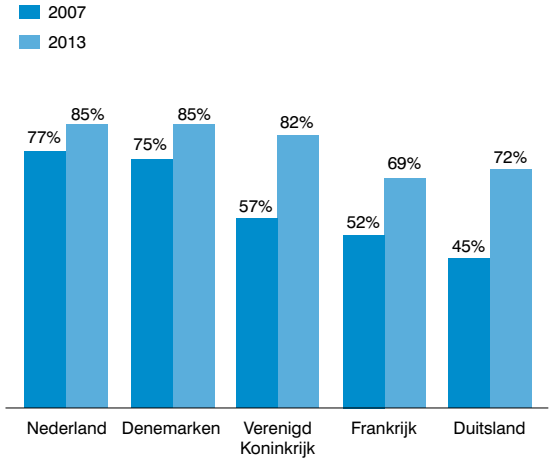
De huidige migratie van breedbandnetwerken naar Next Generation Toegangsnetwerken (NGA) zal de ontwikkeling van de digitale wereld nog versnellen. NGA-netwerken van kabelproviders (gebaseerd op EuroDOCSIS 3.0 technologie) bestaande telecommunicatie

Figuur 1: *Internet gebruikers wereldwijd (in miljoenen)*



Bron: Economist Intelligence Unit

Figuur 2: *Breedbandpenetratie (percentage van huishoudens)*



Bron: OECD

(XDSL), mobile operators en plaatselijke FTTH-netwerken, in combinatie met draadloze clusters zoals digital terrestial- netwerken en satelliet, zullen tegemoet komen aan de vraag naar verhoogde breedbandsnelheden, algemene connectiviteit en geïndividualiseerde mediaconsumptie in alle platforms.

Door de beschikbaarheid en de mate van acceptatie van het internet is de breedbandpenetratie in veel Europese landen hoger dan 70 procent en heeft het de status van massaproduct bereikt vergelijkbaar met andere media, zoals televisie en radio. Hierdoor verandert ook het consumentengedrag: steeds meer consumenten willen altijd en overal contact kunnen maken met de door hen gekozen dienst, met de beschikbare apparatuur.

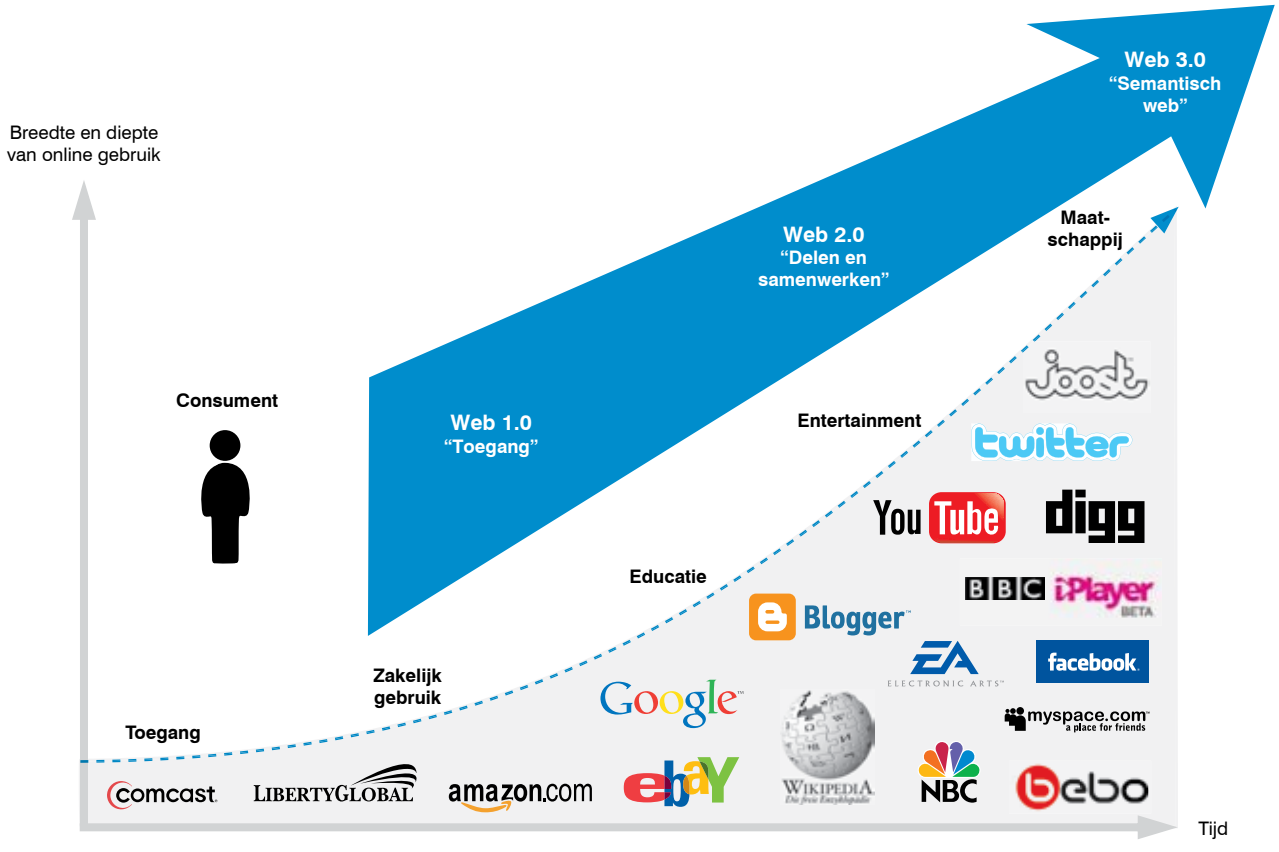
Consumenten veranderen hun gedrag; ze zijn niet alleen meer online, maar ook interactiever online – in sociale netwerken waar ze content en ideeën kunnen uitwisselen. Aan de kant van de leveranciers wordt bij een vergelijking van traditionele mediabedrijven met nieuwe digitale giganten meteen duidelijk waar de groei de afgelopen jaren zich bevond (figuur 4). En zelfs binnen die traditionelere mediabedrijven was de online-groei relatief snel: News Corp., met sterke digitale activiteiten zoals MySpace, is een goed voorbeeld.

2. DE DIGITALE WERELD: EEN BEPALENDE KRACHT IN HEDENDAAGSE ECONOMIE, POLITIEK, MAATSCHAPPIJ EN EDUCATIE

Tot op heden is de groei in internetgebruik vooral gestimuleerd door de inzet van nieuwe technologieën. Apparatuur voor de eindgebruiker zoals pc's en mobiele apparaten bieden goedkope toegang en opslagplatforms. Breedbandnetwerken maken plaats voor ultrasnelle next-generation netwerken. Alle relevante infrastructuren bieden hoge capaciteit (standaard-breedband rond 5 Mbps en in meer ontwikkelde landen tot 25 of zelfs 100 Mbps), in combinatie met interactieve mogelijkheden en altijd beschikbare functionaliteit. Tenslotte hebben MNO's (mobiele netwerkoperators) in Europa mobiel internet met de wijdverspreide beschikbaarheid van 3G geïntroduceerd.

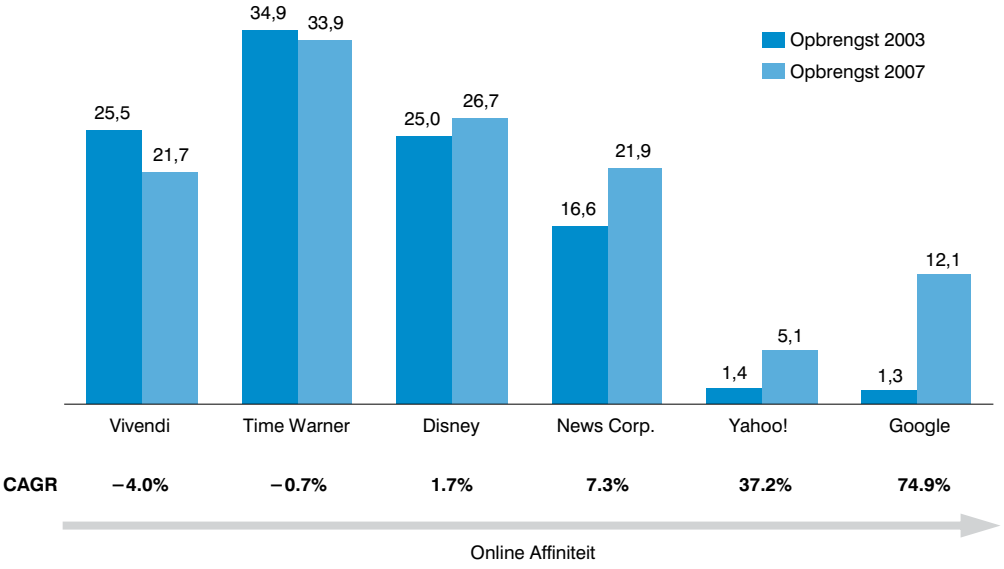
In veel markten is door de huidige technologische voorzieningen vrijwel volledige internettoegang mogelijk. De volgende digitale groeifase

Figuur 3: *Evolutie van de digitale wereld*



Bron: Booz & Company

Figuur 4: *Opbrengsten mediabedrijven met online-bedrijven (in miljarden euro's)*



Bron: OneSource, Bedrijfsrapportages

zal dan ook eerder worden aangedreven door exploitatie van bestaande technologieën dan door de verdere marktpenetratie. Dat betekent dat het gebruik of het gebruikersgedrag zal veranderen en niet zozeer dat het aantal gebruikers toenemen. En dat zien we nu al in veel markten gebeuren. Consumentengedrag verandert drastisch: de belangrijkste informatiebron voor het kopen van een auto is het internet; ongeveer de helft van de boeken in de Verenigde Staten wordt online verkocht via Amazon en kabeloperator Comcast registreert een dergelijke 40 miljoen filmdownloads per maand.

Sectoren veranderen door het internet – Amazon verkoopt voor meer dan $4,5 miljard boeken in de Verenigde Staten. Dat is bijna de helft van het totaal, vergelijkbaar met Barnes & Noble in traditionele verkoop.

Als antwoord op de veranderende patronen in mediaconsumptie maken bedrijven dankbaar gebruik van de kracht van het internet voor reclame en marketing – in Groot-Brittannië wordt bijvoorbeeld meer dan 15 procent van reclamegeld online besteed.

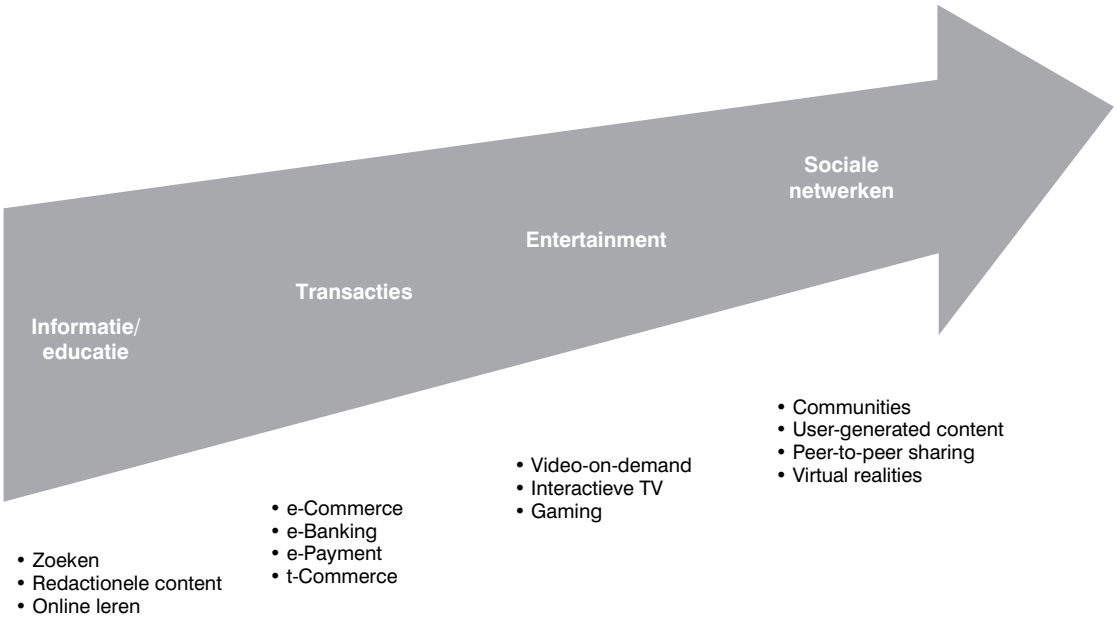
Het internet en de digitale omgeving in het algemeen zijn een zeer aantrekkelijk platform geworden voor diverse reclame- en marketingactiviteiten. Ten eerste besteden consumenten steeds meer tijd aan digitale media en ten tweede hebben digitale media grote voordelen zowel in efficiency als in effectiviteit vergeleken met andere reclamemiddelen – een essentieel punt. Veel geraffineerde reclamevormen, met name degene die hun relevantie voor de individuele consument willen vergroten, kunnen alleen worden ingezet als de digitale media een rijkdom van gebruik- en gebruikersinformatie kunnen exploiteren.

Zo krijgen gebruikers van Google Gmail reclame te zien die is afgestemd op de inhoud van hun e-mails. Op dezelfde manier kunnen browsergeschiedenis, actief beheerde profielen en andere data gebruikt worden voor om reclame af te stemmen op de individuele consument. Ook bij digitale tv kunnen gebruik- en gebruikersgegevens worden gevolgd via de set-top box en gebruikt om gerichte reclame te tonen aan specifieke segmenten of individuele gebruikers. En met interactieve DTV biedt reclame dezelfde interactieve responsmogelijkheden als online.

Adverteerders spenderen steeds meer aan het internet – online adverteren is goed voor 15 procent van de totale adverteerdersmarkt in Groot-Brittannië.

Goede privacybescherming is een zeer belangrijk aspect voor de consument dat met grote zorg moet worden aangepakt, zelfs als gegevens over het internetverkeer van de gebruiker op samengevoegd, anoniem niveau worden gebruikt voor commerciële doeleinden. Maar hoe opdringerig het op het eerste gezicht ook lijkt, de ervaring leert dat gerichte reclame, op de juiste manier ingezet, de gebruikersacceptatie kan vergroten, omdat de reclame relevant is voor de consument. Bovendien zijn er veel manieren om zulke reclame vorm te geven, zodat ongewenste participatie wordt voorkomen: via opt-in/opt-out

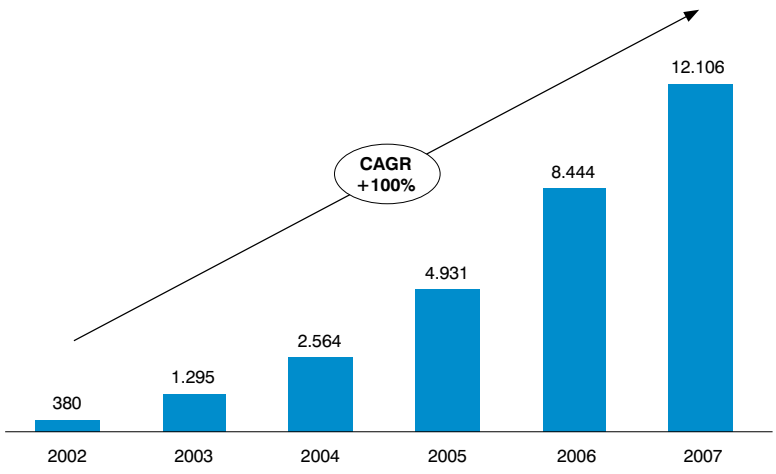
Figuur 5: *Digitale wereld – groeifactoren*



procedures kunnen gebruikers bepalen dat hun gegevens niet worden gebruikt voor gerichte reclame – maar zij kunnen dan wel steeds vaker gevraagd worden te betalen voor het verlies aan inkomsten aan adverteerderszijde. Verder zal reclame de belangrijkste financier van veel diensten en aanbiedingen in de digitale omgeving blijven, zoals dat in de traditionele media al decennia het geval is.

Tegen deze achtergrond en gezien de ervaringen met de digitale economie gedurende de laatste vijftien jaar, zal reclame in brede zin waarschijnlijk een van de grootste inkomstencategorieën zijn in de toekomstige groei van de digitale economie. Het beheren van de waargenomen en daadwerkelijke opdringerigheid voor de digitale wereld is een eerste vereiste om die groei te bewerkstelligen. Zeker gezien de toenemende druk om nieuwe Web 2.0-diensten te gelde te maken, wordt dit een van de grootste uitdagingen voor alle betrokkenen in de bedrijfstak.

Figuur 6: *Groei van Google (opbrengsten in miljoenen euro's)*



Bron: Google

Wat toepassingen betreft zien wij vier belangrijke groei-instrumenten voor de digitale wereld:

- **Informatie en educatie.** De traditionele Web 1.0-toepassingen in combinatie met Web 2.0-tweaks zoals user-generated content, bijvoorbeeld in e-learning.

- **Transacties.** Voornamelijk e-commerce en online bankieren.

- **Entertainment.** Digitale tv, videodiensten (streaming video en video-on-demand zoals YouTube) en gamen, evenals downloadservices zoals iTunes.

- **Sociale Netwerken.** Alle diensten rond menselijke interactie, bijvoorbeeld in gemeenschappen het uitwisselen van hoofdzakelijk door gebruikers samengestelde content of ontmoetingen in virtuele omgevingen.

INFORMATIE EN EDUCATIE

Informatie – met name zoeken – is vanaf het begin een van de grootste groeifactoren van de groei in internetgebruik. Zoekmachines hebben opmerkelijke successen geboekt in het vertalen van de overvloed van beschikbare data op het

net in zinvolle informatie voor eindgebruikers. Het internet vergemakkelijkt ook samenwerking en biedt consumenten educatie en voorlichting door bijvoorbeeld user-generated content en ideeën zoals Wikipedia – dat meer dan tien miljoen user-generated artikelen in 250 talen bijeen heeft gebracht. Sinds de lancering in 2001 ontwikkelt Wikipedia zich tot de meest geraadpleegde bron voor (encyclopedische) informatie. Daarmee is het een van de belangrijkste educatie- en onderzoekshulpmiddelen geworden – wat zelfs de vraag oproept of studenten nog wel in staat zijn "echt" onderzoek te doen aan een bureau in de bibliotheek. Het open en gemeenschappelijke karakter van Wikipedia, zowel qua user-generated content als de controle op de inhoud door de gebruiker, maakt het een uitstekend voorbeeld van een echte Web 2.0-toepassing die het "informatieheelal" binnentreedt. Volgens sommigen zou Wikipedia door het dynamische karakter bovendien nauwkeuriger zijn dan veel andere, statische informatiebronnen.

Meer dan 45 procent van de bedrijven maakt regelmatig gebruik van internet-gebaseerde training

Digitale tv is een andere belangrijke aandrijfkracht van het informatietijdperk. Het aantal televisiezenders in Europa is inmiddels een verbijsterende 1.703 (in 2005), waar het 18 jaar geleden met slechts 93 zenders begon. Veel van de voor consumenten beschikbare zenders bieden nieuws, documentaires of programma's in vreemde talen die in de analoge wereld niet bestonden of niet toegankelijk waren.

Universiteiten en andere hogere onderwijsinstellingen maken steeds meer gebruik van de mogelijkheden van het internet om effectief informatie te verspreiden en handige, zinvolle interactie mogelijk te maken met oplossingen zoals WebEx (voor web-conferencing en -samenwerking). Vooral het onderwijs op afstand, waar vijftien jaar geleden veel fysieke taken bij kwamen kijken (reizen, opgaven insturen) maakt veel gebruik van de mogelijkheden. Verscheidene universiteiten en hogescholen (Open University in Groot-Brittannië, bijvoorbeeld) begonnen Second Life te gebruiken als een virtueel klaslokaal. Bedrijven gebruiken het internet en verwante digitale media ook om hun werknemers te trainen, in de vorm van webcasts of web-based training (WBT), een uitbreiding van de traditionele computer-based trainingen (CBT).

Informatie en educatie zullen de groei van de digitale wereld in belangrijke mate stimuleren. Met name zoekopdrachten ondersteund door bijpassende online-reclame sterk blijven toenemen. Google, het rolmodel voor het vertalen van zoekopdrachten in reclameopbrengsten, heeft gedurende de afgelopen vijf jaar een totale jaarlijkse opbrengstgroei gerealiseerd van meer dan 100 procent door het agressief marketen van zijn businessmodellen en haar aanbod dynamisch te blijven vernieuwen en zo een publiek te bereiken dat meer dan twee keer zo groot is als dat van de grootste Europese televisiemaatschappij, de RTL groep.

TRANSACTIES

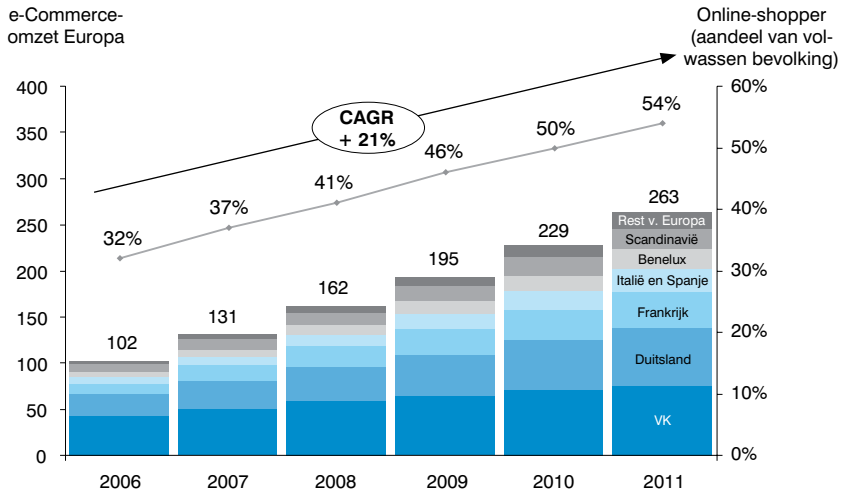
Het internet heeft bewezen het ideale medium te zijn voor transacties.

Door online te winkelen profiteren consumenten onder andere van concurrerende prijzen dankzij vergelijkingssites. Momenteel winkelt meer dan 40 procent van de consumenten online en aan e-commerce wordt in Europa jaarlijks meer dan €150 miljard besteed, een toename van rond de 50 procent in de afgelopen twee jaar. Uitgaven in e-commerce bedragen op dit moment meer dan 4 procent van de totale Europese verkopen in retail, met een verwachte groei van 11 procent in 2011. Voor bepaalde producten, zoals evenemententickets, reizen en media (boeken, muziek, video en software), wordt voor 2011 een aandeel verwacht van 25 tot 35 procent.

Meer dan 40 procent van de consumenten winkelt online en e-commerce is momenteel goed voor meer dan 4 procent van de totale Europese retailverkopen

Daarnaast heeft het internet de manier waarop consumenten hun financiën beheren gerevolutioneerd door digitale transacties mogelijk te maken. Het internet is erin geslaagd een aanzienlijk

Figuur 7: *B2C e-Commerce omzet Europa (miljarden euro's)*



Bron: Forrester

niveau van vertrouwen te scheppen in haar – in het algemeen solide – veiligheid; en internetbankieren heeft zich ontwikkeld tot een massafenomeen. En gelijk met de groei van internettransacties is er een brede reeks betalingsoplossingen ontstaan zoals PayPal, om tegemoet te komen aan de toenemende behoefte om online goederen en diensten te kopen. Vanwege de bijzondere gevoeligheid van financiële transacties zijn er echter zorgen over de veiligheid ervan.

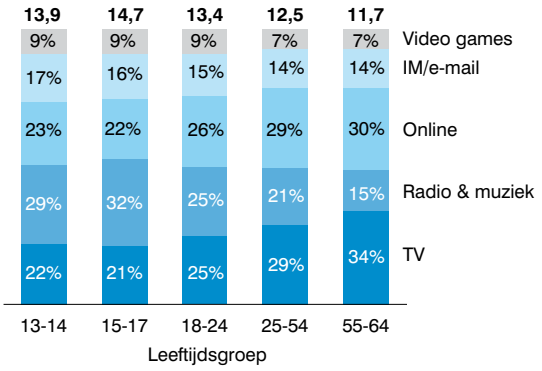
Er zijn nieuwe bedrijven gekomen die de kans aangrijpen om uitsluitend via internet te werken in een virtueel businessmodel, voor een fractie van de kosten van een fysieke onderneming; zij zetten de kracht van het internet in als een verkoopkanaal met lage kosten en een efficiënte methode voor de bevoorrading van de leveringsketen. Fysieke bedrijven profiteren eveneens van een extra, goedkoop platform voor klantenservice en betalingen – waarbij ze vaak extra kosten berekenen voor klanten die de internetdienst niet willen gebruiken. Mobiele operators introduceerden bijvoorbeeld al enige jaren geleden de zogenaamde "internet only" aanbiedingen.

ENTERTAINMENT

De meest ingrijpende verandering in de digitale wereld voor de meeste consumenten ligt waarschijnlijk op het gebied van entertainment. De gemiddelde Europese consument kijkt tussen de 160 en 240 minuten televisie per dag en tot 140 minuten op het internet – steeds vaker ook voor entertainment. Alles bij elkaar is het gebruik of verbruik van interactieve media qua bestede tijd veruit de belangrijkste vrijetijdsbesteding in Europa. En dit is drastisch aan het veranderen. Het internet wordt nu al de toonaangevende mediavorm in veel ontwikkelde economieën, waar mensen meer tijd online en aan e-mail besteden dan aan televisiekijken (figuur 8).

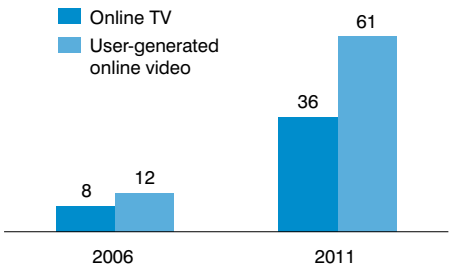
Consumenten hebben het steeds drukker en zoeken daarom naar entertainment-aanbod "on-demand", waar ze kunnen kijken wat ze willen, wanneer ze dat willen en hoe ze dat willen. Met de toegenomen capaciteit van breedband-

Figuur 8: ***Tijd besteed aan media per dag, VS 2007 (uren per dag)***



1) Verenigde Staten
Bron: eMarketer

Figuur 9: ***Online videostreams VS (in miljarden)***



Bron: eMarketer

netwerken kunnen diensten als video-on-demand tegen gunstige prijzen worden geleverd.

Digitale televisie gaat de televisiebelevenis van de consument revolutionair veranderen. In de afgelopen jaren zagen we een ware explosie van het aantal tv-kanalen (en de diversiteit daarin) en werden veel regionale en themazenders toegevoegd. Bovendien is met HDTV de beeldkwaliteit aanzienlijk beter geworden. DTV introduceerde ook een aantal echt nieuwe functies zoals video-on-demand en de mogelijkheid om een programma op een later tijdstip bekijken – "time-shifted tv" – en ondersteuning voor speciale functies zoals interactiviteit en elektronische programmagidsen.

Daarnaast komen er commerciële platforms die gebruikmaken van de grotere capaciteit van breedbandnetwerken om multimediadiensten via het internet aan te bieden – zo verzorgt in Groot-Brittannië de BBC iPlayer tv-shows en radio over het internet.

Meer dan de helft van de internetgebruikers in de Verenigde Staten (57 procent) gebruikt internet om online video's te bekijken en bijna 20 procent doet dat elke dag. En deze percentages liggen nog hoger voor breedbandgebruikers (74 procent bekijkt video's online). Vorig jaar waren zijn een aantal starters opgekomen die van internet echte televisie willen maken: Joost, Babelgum en andere bieden televisie van hoge beeldkwaliteit, verrijkt met Web 2.0-elementen in een zogeheten "over-the-top"- (OTT) aanpak, "boven op" een kabel- of telecomnetwerk zonder liaison met de netwerkprovider.

Deze trends maken het internet niet alleen een belangrijker medium voor reclame; ze maken het ook een belangrijke "vormgever" van de

publieke opinie. Voorstanders van vrijheid van meningsuiting en een goed geïnformeerd publiek (politiek, sociale wetenschappen en culturele instanties) zullen steeds meer belangstelling tonen voor deze veranderingen in "mediaconsumptie".

SOCIAAL NETWERKEN

Door sites voor sociaal netwerken zoals Facebook en Bebo is er steeds meer maatschappelijke interactie. Deze bieden aan de ene kant functies die er zonder het internet niet zouden zijn en laten mensen online vriendschappen onderhouden, ongeacht de fysieke afstand. Aan de andere kant ontstaat door deze functies ook enige angst over wat er gebeurt met traditioneel maatschappelijk gedrag, zoals persoonlijke, face-to-face interactie en vriendschap.

Sociaal gedrag verandert – mensen maken sneller contact en met meer sociale groepen als ze het internet gebruiken

Sociaal netwerken is een relatief recent fenomeen dat bijdraagt aan de algemene Web 2.0-trend richting online maatschappelijke gemeenschappen. Gebruikers – met name die van de "born digital" generatie – maken deel uit van interessegroepen in een online context, die online content genereren, publiceren en delen. Steeds meer internetgebruikers maken gebruik van sociaal netwerken; de meesten bezoeken meerdere sites regelmatig.

Al vrij lang beïnvloedt het internet het maatschappelijke gedrag van consumenten. Volgens een in 2004 gehouden onderzoek in de Verenigde Staten, "Social Ties", onderhield de gemiddelde internetgebruiker meer regelmatige contacten (37 voor internetgebruikers versus 30 voor niet-internetgebruikers). Meer dan 30 procent van de internetgebruikers zei bovendien dat ze door het internet meer contacten en kennissen hadden.

MAATSCHAPPELIJKE VERANDERINGEN

Zoals boven uiteengezet en verder uitgewerkt in dit rapport, is digitale technologie vandaag al een belangrijke economische kracht – en meer nog in de toekomst. Maar dit moet niet alleen als een economische factor worden bekeken.

Het internet bepaalt steeds meer de opinievorming – Google wordt vaak gezien als een van de meest betrouwbare nieuwsbronnen wereldwijd, meteen na CNN en de BBC

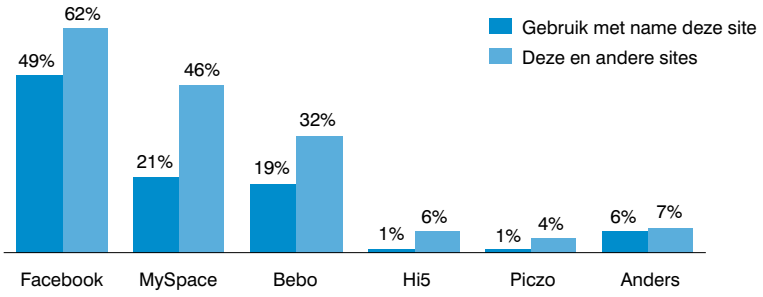
Het internet in het bijzonder en digitale diensten in het algemeen zullen veranderingen teweegbrengen die veel verder reiken dan de verkoop van boeken of vliegtickets. Digitale technologieën stellen iedereen in staat gehoord te worden en contact te leggen met een breed publiek, in welke context dan ook.

Politici gebruiken het internet om zichzelf en hun ideeën te presenteren, om van gedachten te wisselen met hun aanhangers en om hun campagnes te organiseren. De Amerikaanse presidentskandidaat Barack Obama maakt bijvoorbeeld uitvoerig gebruik van sociaal netwerken voor zijn presidentiële campagne. Op "Twitter" heeft hij meer 30.000 "followers", die regelmatig korte updates van hem ontvangen. Momenteel gebruikt bijna een kwart van de Amerikanen het internet regelmatig als bron van politieke/campagne-informatie. Bij 18- tot 29-jarigen is dat zelfs meer dan 40 procent. Obama heeft het gebruik van internet als politiek instrument een extra dimensie gegeven: hij gebruikt het om fondsen te werven voor zijn campagne.

De maatschappij is er door het internet anders uit gaan zien – zo kan 60 procent van de VS-consumenten zonder telefoon, maar slechts 55 procent zonder internet

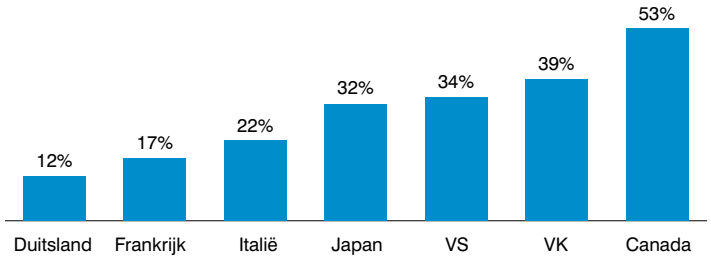
Meer dan één miljoen mensen droegen gemiddeld $105 bij – tien jaar geleden een onmogelijk concept, maar nu een belangrijke inkomstenbron.

Figuur 10: *Gebruik sociale netwerken door volwassenen (VK [1], 2007, percentage gebruikers sociale netwerken)*



1) Verenigd Koninkrijk
Bron: Ofcom

Figuur 11: *Gebruik sociale netwerken door volwassenen (2007, percentage internetgebruikers per land)*



Bron: Ofcom, Nielsen
n=391

De “born digital” generatie – Digital Confidence treedt op de voorgrond

Kinderen en jeugd in geïndustrialiseerde landen zijn de eerste generatie geboren in een digitale wereld. Zij zijn de early adopters van nieuwe technologie en in vergelijking met hun ouders IT-specialisten. En tot op heden worden slechts delen van de oudere generatie “hergeboren” in dit digitale leven.

Wired Magazine schrijft over “born digital”:

- Een zelfkarakterisering: “We leerden achter de pc te kruipen. We groeiden op met het internet. We waren early adopters, op alle mogelijke manieren connected en altijd online.”

- Over technologie: “Van IM naar mp3 naar P2P... we doen labtests voor de cultuur van morgen. Terwijl anderen zich verbazen over de digitale toekomst, vinden wij het heel normaal. Zie het als het verschil tussen een tweede en een eerste taal.”

De “born digital” generatie maakt geen onderscheid tussen on- en offline zoals veel volwassenen meestal doen – zij ziet beide “werelden” als veel meer onderling verbonden; ze leven in echte én in virtuele communities, met vaak een forse overlapping binnen hun leeftijdsgroepen. En ze hebben hun eigen “online” cultuur, taal en netiquette.

Maar de “born digital” generatie zorgt ook voor wat uitdagingen, zowel voor zichzelf als voor de rest van de maatschappij.

- Wat een paradox: ze zetten zichzelf uitvoerig te kijk op sites voor sociaal netwerken, geven bereidwillig hun privacy op, maar reageren heftig als ze vinden dat hun gegevens worden misbruikt – zoals gebeurde in de Facebook Beacon-zaak, waarbij meer dan 50.000 gebruikers in december 2007 een petitie tekenden met klachten dat een programma plannen zou hebben om Facebook samen te laten gaan met externe partnersites om zo gericht te adverteren.

- Ouders en scholen (de “natuurlijke opvoeders”) zijn overbezorgd over de reikwijdte van nieuwe fenomenen en de snelheid van innoveren.

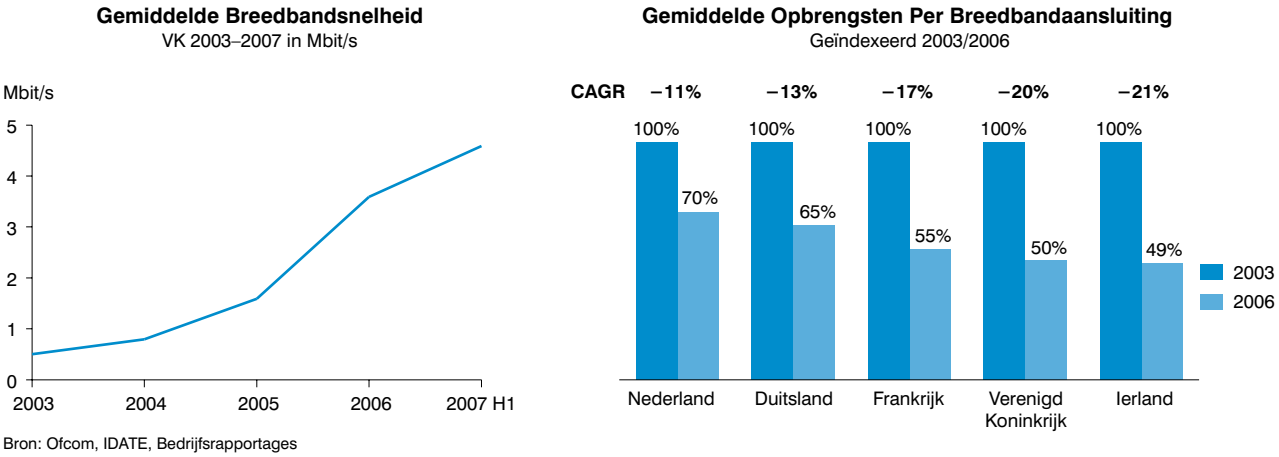
- Traditionele juridische normen en waarden zijn lastiger toepasbaar op “dubbelzinnige” digitale activiteiten en worden minder geaccepteerd, bijvoorbeeld wat betreft het delen van content onder auteursrecht.

In het algemeen wordt de “born digital” generatie onvoldoende begeleid in passend gedrag in digitale omgevingen, wat druk legt op businessmodellen: al vele jaren in het geval van copyright, maar ook in de toekomst als de bedrijfstak nieuwe businessmodellen voor reclame probeert te implementeren.

Blogs, podcasts, chatsites, gebruikersfora, nieuwsgroepen en andere geavanceerde online communicatie- en publicatiemiddelen hebben niet alleen de communicatie binnen organisaties om hun doelstellingen te bereiken en andere communicatiebehoeften veranderd; omdat communicatie zoveel gemakkelijker is geworden, worden geruchten en nieuws ook sneller en uitvoeriger verspreid. Een van de consequenties daarvan is dat organisaties ook veel vaker een informatie- en communicatiebeleid moeten ontwikkelen en toepassen, met name inzake vertrouwelijke bedrijfsinformatie. Opiniesites zoals “ciao” – actief in meerdere Europese landen met meer dan 38 miljoen bezoekers per maand – en blogs hebben een werkelijk nieuwe informatiebron gecreëerd die geraadpleegd wordt alvorens een dienst of product aan te schaffen, wat zowel sterk in het voordeel als in het nadeel van individuele marketeers, serviceproviders, retailers en dergelijke kan werken. De kracht van blogs en online syndicaatvorming reikt veel verder dan e-commerce alleen en de digitale wereld zelf: Kate Hanni, een zeer ontevreden passagier van American Airlines, stichtte The Coalition for an Airline Passengers’ Bill of Rights om vliegtuigpassagiers rechten te geven. Dat deed ze samen met een aantal medeslachtoffers nadat ze met meerdere vliegtuigen van American Airlines meer dan negen uur waren gestrand op het Austin International Airport in december 2006, “zonder water of mogelijkheid van toiletruimtes gebruik te maken”. Deze coalitie heeft nu meer dan 20.000 leden, maakt gebruik van een website en een blog om “horror stories” uit te wisselen en laat van zich horen – ze hebben het Amerikaanse Congres regelmatig bezocht en momenteel staan wetgeving en veranderingen in regulering ter discussie om dergelijke gevallen in de toekomst te voorkomen.

De kracht van het Web 2.0-dienstenaanbod, zoals opiniesites en gebruikersoordelen is terug te vinden in de Trust Barometer van Edelman: de 2008-editie meldt dat in veel landen, inclusief de Verenigde Staten, Nederland en Duitsland, “iemand als ik” wordt gezien als de meest betrouwbare informatiebron voor de beoordeling van een bedrijf, nog veel meer dan enige officiële informatiebron, de CEO inbegrepen.
In alle onderzochte landen zeiden vier van de vijf respondenten dat ze “veel eerder geloven wat ze zien, lezen of horen over een bedrijf als een bekende het al heeft gezegd”. Gewoontegetrouw worden NGO’s (non-gouvernementele organisaties) als het betrouwbaarst beschouwd, vergeleken met bedrijven, media en de regering – in de Verenigde Staten, Duitsland en Frankrijk staan NGO’s ver bovenaan.

Figuur 12: ***Het breedband dilemma***



Bron: Ofcom, IDATE, Bedrijfsrapportages

Velen staan verbaasd over de snelheid waarmee de digitale wereld verandert. Tezelfdertijd is er een nieuwe generatie "born digital" voor wie de mogelijkheden van de digitale wereld net zo gewoon zijn als de radio dat 50 jaar geleden voor de meeste mensen was. Zij gebruiken nieuwe technologieën als eersten en zijn IT-specialisten vergeleken met hun ouders; ze maken geen onderscheid tussen online en offline zoals veel volwassenen, maar leven meer in echte zowel als virtuele gemeenschappen die elkaar vaak binnen hun leeftijdsgroep overlappen. En ze hebben hun eigen "online"-cultuur, taal en netiquette. Toch stelt de "born digital" generatie ons ook voor belangrijke uitdagingen omdat ze geen richtlijnen krijgen over passend gedrag met betrekking tot het delen van persoonlijke gegevens of auteursrechtelijk beschermde content. Dit is niet alleen lastig voor henzelf en daardoor een opvoedingstaak voor de maatschappij, maar ook een reëel probleem voor digitale businessmodellen, bijvoorbeeld in digitale content en innovatieve reclame. De bedrijfstak moet een gemeenschappelijke mening vormen over het omgaan met de "born digital" generatie en nieuwe manieren vinden om samen te werken.

De volgende groeifase in de digitale economie wordt eerder veroorzaakt door meer gebruik dan door meer gebruikers

CONCLUSIE

De in kaart gebrachte drijfkrachten van de digitale wereld zorgen voor grote veranderingen in alle lagen van het bedrijfsleven en de maatschappij. Zeker is dat de digitale wereld de economische groei en de welvaart zal blijven stimuleren en een grotere rol in ons dagelijks leven zal gaan spelen. Door de digitale infrastructuur ontstaan nieuwe vormen van onderling contact, communicatie en zakendoen die nog nauwelijks worden geëxploiteerd.

3. AANDRIJVERS VAN INKOMSTEN EN GROEI: CONTENT EN RECLAME, NIET TOEGANG

De in kaart gebrachte groeigebieden zorgen voor toenemende opbrengsten voor de digitale economie in de volgende vier categorieën:

1. Reclame. Alle vormen van online-reclame, inclusief doorklik-opbrengsten[1)], IPTV-reclame en sponsors (bijvoorbeeld online programmasponsoring; "Deze show wordt u aangeboden door xxx").

2. Content. Digitale online content, inclusief video-on-demand, gaming, tv (betaalde webtelevisie en streaming video) en muziek downloads.

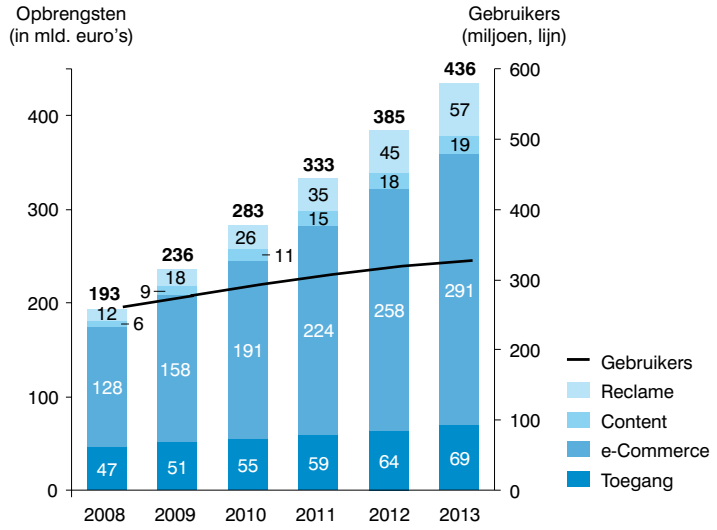
3. e-Commerce. Producten en diensten die via het internet worden besteld en op traditionele wijze worden bezorgd (bijvoorbeeld boeken van Amazon en vliegtickets van vliegmaatschappijen).

4. Toegang. Transport van dataverkeer naar het internet en toegang tot digitaal tv-aanbod, met name de inkomsten van netwerkoperators (kabel en DSL) voor het leveren van internettoegang.

e-Commerce is de meest gevestigde en grootste inkomstencategorie. Onlinereclame en content zijn relatief nieuwe inkomstencategorieën, met een groei van respectievelijk 32 procent en 22 procent, hoewel ze laag begonnen (figuur 13).

1) Doorklikopbrengsten staan voor volumegebaseerde betaling aan een zoekmachine voor een gesponsorde link naar een website

Figuur 13: *Europese online opbrengsten en gebruikers*



Noot: Europa inclusief EU-26, Noorwegen en Zwitserland
Bron: Forrester e-Commerce Forecast, Bedrijfsrapportage Apple, Bedrijfsrapportage Google, EU TV and Broadband Forecast Model, Booz & Company analyse

Tot op heden is de digitale economie in hoge mate bepaald door technologische vooruitgang; de migratie naar breedbandnetwerken zorgde voor een explosief toegenomen internet-penetratie en -gebruik. Breedbandtoegang is nu een massamarkt-fenomeen in veel Europese, Aziatische en Amerikaanse landen.

De totale markt voor de "digitale wereld" groeit met 18 procent per jaar, wat een volume van €436 miljard betekent

In sommige landen, met name in West-Europa, is het punt van verzadiging bijna bereikt, terwijl sommige landen in Zuid- en Oost-Europa achterblijven. Verwacht wordt dan ook dat de toegangsopbrengsten in deze landen stabiel zullen blijven. Gelijktijdig wordt de transportinfrastructuur steeds meer een commercieel product door een zeer competitieve markt met gevestigde technische oplossingen en weinig ruimte voor differentiatie.

Toegangsmarges staan onder druk door afnemende groei van het aantal abonnees en matige groei van toegangsopbrengsten, in combinatie met de toenemende vraag naar meer bandbreedte (bijvoorbeeld video-on-demand, P2P). Het algehele waardeaandeel van toegang zal afnemen van de huidige 24 procent naar minder dan 16 procent rond 2012.

Er komt een aanzienlijke waardeverschuiving, weg van de infrastructuur: het aandeel van toegangs-business in de digitale wereld zal de komende vijf jaar fors dalen – 16 procent in 2012 vs. 24 procent vandaag

Terwijl de opbrengsten de komende jaren naar verwachting sneller zullen toenemen dan het aantal gebruikers (totaal 18 procent jaarlijkse groei van opbrengsten tegen 4 procent groei van gebruikers) is er bewijs voor een fundamentele waardeverschuiving in de hele waardeketen. Toekomstige groei zal komen van toenemende opbrengsten door het gebruik per individu te stimuleren, meer dan door toename van het aantal gebruikers. Naar verwachting zal deze groei veroorzaakt worden door innovatievere producten en diensten, aangevuld met nieuwe businessmodellen die ook opbrengsten genereren.

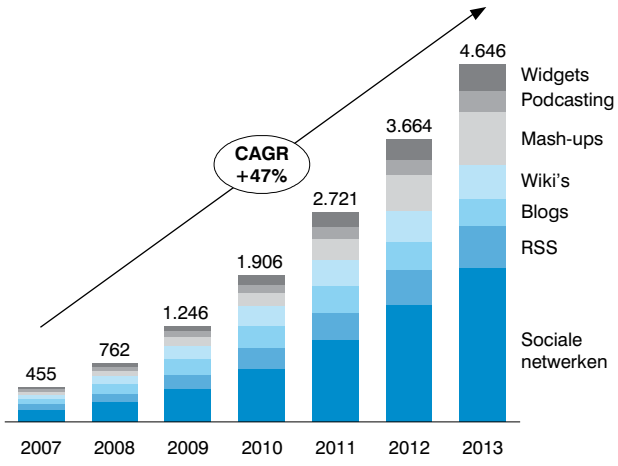
Netwerkoperators, die de digitale wereld mogelijk maken, moeten meer dataverkeer ondersteunen voor minder inkomsten

Deze nieuwe diensten hebben betrekking op zowel consumenten als zakelijke omgevingen. Forrester schat bijvoorbeeld dat Web 2.0-gerelateerde B2B-verkopen zullen groeien met 47 procent per jaar, met als resultaat bijna $5 miljard in groei wereldwijd rond 2013.

Netwerkoperators moeten nieuwe businessmodellen en waarde creëren door diensten en toepassingen in plaats van vergroten van toegang – ook moeten ze investeren in NGN's om groei te verwerven en waarde-toevoegende diensten te kunnen bieden

Dientengevolge zal de volgende groeifase in de digitale economie worden aangedreven door diensten en toepassingen die alleen gerealiseerd kunnen worden in lijn met de breedbandpenetratie per land. In landen waar de breedbandinfrastructuur nog niet geheel is ingevoerd blijft breedbandaanleg dan ook de belangrijkste basis voor groei van de

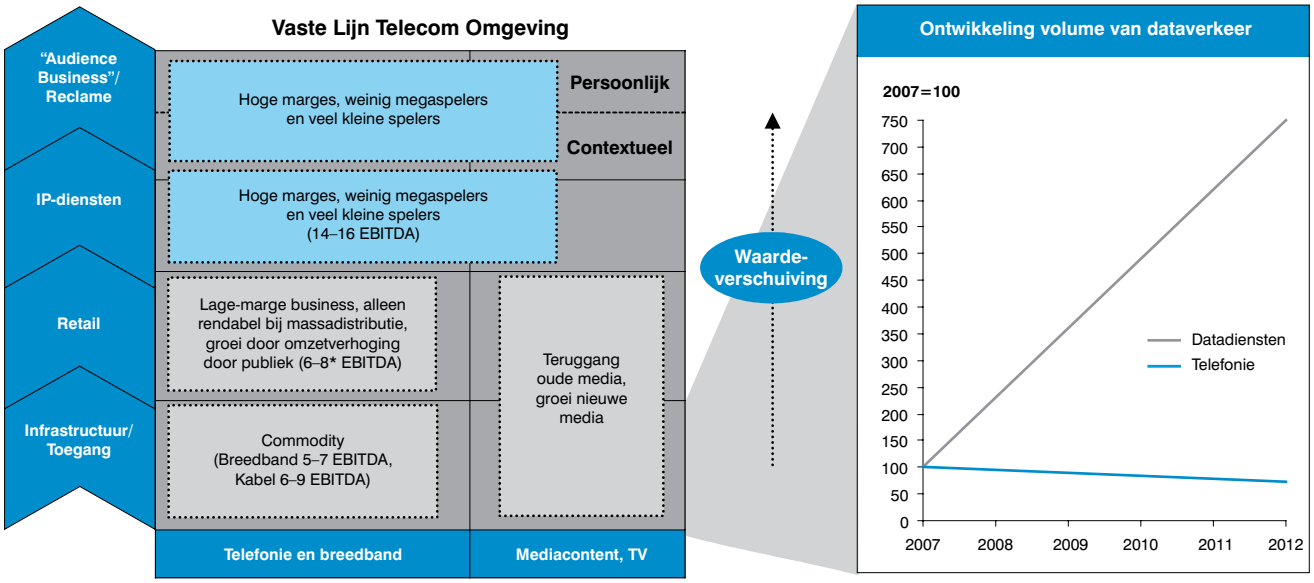
Figuur 14: *Wereldwijde jaarlijkse omzet Enterprise 2.0 (miljoenen US dollars)*



Bron: Forrester

digitale economie. In landen waar breedband al volwassener is, dienen netwerkoperators conversie van next generation netwerken (NGN's) te blijven stimuleren om voorbereid te zijn op de te verwachten overvloed aan dataverkeer door toenemend gebruik in het algemeen en introductie van tv met hoge beeldkwaliteit en video in het bijzonder.

Figuur 15: *Visie op dataverkeer*



Noot: Europa 27+2 (Zwitserland, Noorwegen), d.w.z. inclusief minder ontwikkelde breedbandmarkten; conservatieve schatting voor ontwikkelde markten
Bron: Ovum, Booz & Company analyse

III. DIGITAL CONFIDENCE: SLEUTEL TOT DE DIGITALE GROEI VAN MORGEN

1. BEDREIGINGEN VOOR DE DIGITALE WERELD

De groei van onze digitale wereld kan duurzaam zijn door een continue toename van online gebruik en besteding. Om dit te bereiken moeten gebruikers en bedrijven vertrouwen hebben in de omgeving waarin ze opereren. Gebruikers moeten informatie krijgen over de potentiële gevaren en leren hoe met deze gevaren om te gaan – ze moeten zich veilig voelen en ook werkelijk veilig zijn. Een van belangrijkste uitdagingen voor de bedrijfstak is het leveren van veilige netwerkomgevingen en zorgen voor een optimale gebruikerservaring.

Met het succes van de digitale wereld zijn bij gebruikers en bedrijven zorgen ontstaan over de veiligheid en de integriteit van de digitale omgeving

De verspreiding van gebruiksvriendelijke technologieën en onbeperkt verbonden zijn met internet hebben bijgedragen aan de positie van internet als het belangrijkste platform van de digitale wereld. Met strategieën die zich richten op meerdere platforms en "webification" is mogelijk andere typen platforms, zoals digitale televisie en mobiele platforms, op te nemen in het raamwerk.

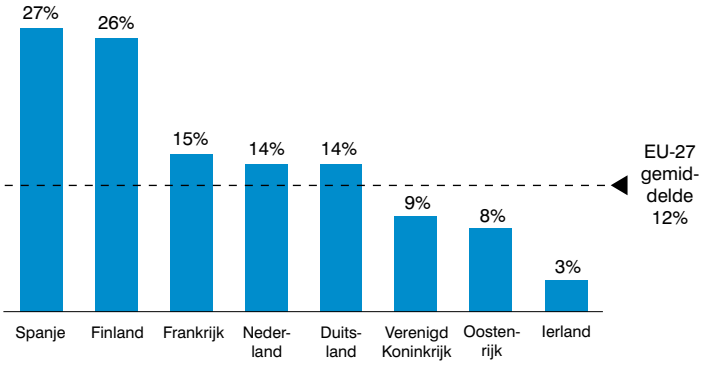
De groei van de Web 2.0-economie geeft reden tot zorg. De eerste zorg komt voort uit de manier waarop de gebruikers zelf omgaan met de toenemende stroom van persoonlijke gegevens over het internet op sites voor sociaal netwerken. De druk op providers en diensten om Web 2.0-toepassingen (voornamelijk sites voor sociaal netwerken) en investeringen in NGN's te gelde te maken, legt steeds meer commerciele druk op consumenten. Bijvoorbeeld door nieuwe, reclamegedreven businessmodellen en andere vormen van gericht adverteren, waarbij gebruik wordt gemaakt van online gebruikersprofielen, blogs en fotoalbums. Dit kan consequenties hebben wanneer toekomstige werkgevers kandidaten scannen.

Andere zorgen houden verband met onbetrouwbare netwerkbeveiliging, waardoor die persoonlijke gegevens niet vertrouwelijk blijken en waardoor diensten die afhankelijk zijn van een veilige netwerkomgeving onder druk komen te staan (figuur 17). Dat deze zorgen terecht zijn, blijkt uit een analyse van de top-10 van internetoplichting in de Verenigde Staten in 2007. De meeste van deze zaken hadden betrekking op e-commerce; per geval betrof het daadwerkelijke verliesposten tot $4000 (figuur 18). 12 procent van de Europeanen koopt niet via het internet, juist omdat men bezorgd is over de beveiliging (figuur 16). Naast fraude krijgt de commercie in toenemende mate te maken met kwaadwillende gebruikers. Data geven aan dat de sector wereldwijd in 2005 al meer dan $1000 miljard verloor aan inkomsten, de kosten van verloren tijd, schade aan systemen en reputatieschade. Tussen 2000 en 2005 zijn deze kosten extreem snel gegroeid als gevolg van de toenemende digitalisering (figuur 19). De huidige jaarlijkse schade is zelfs door experts niet meer in te schatten.

Eén op de acht consumenten is bezorgd over de veiligheid en koopt daarom niet via het internet

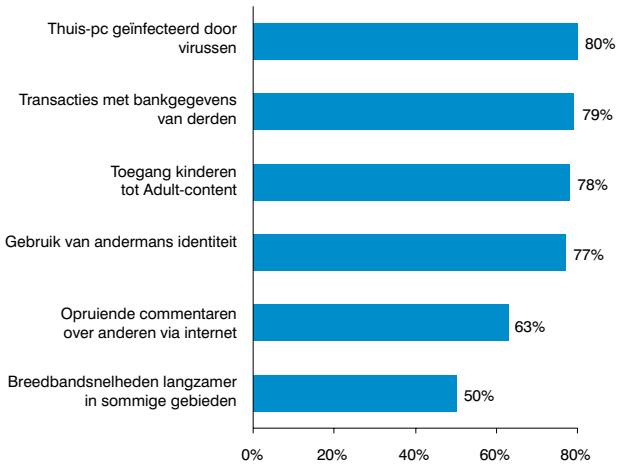
Web 2.0 is ook de belangrijkste ontwrichtende kracht voor de audiovisuele sector door het online illegaal kopiëren en de mening van het grootste deel van de "born digital" generatie dat content gratis zou moeten zijn. De mediasector worstelt met het feit dat traditionele wetgeving niet meer als vanzelf geaccepteerd wordt in de context van "ambigue" digitale activiteit, bijvoorbeeld het delen van auteursrechtelijk beschermde content, zodat de mediasector dringend manieren moet vinden om op effectieve wijze online juridische bescherming af te dwingen en de "digitale

Figuur 16: *Percentage consumenten die e-shopping vermijden door zorgen om veiligheid (Europa, 2007)*



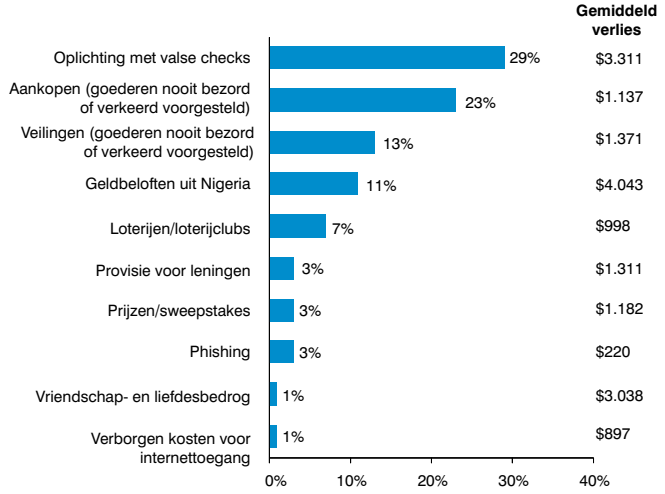
Bron: Eurostat

Figuur 17: *Bekendheid met diverse internetproblemen (onderzoek VK, 2007)*



Bron: Ofcom

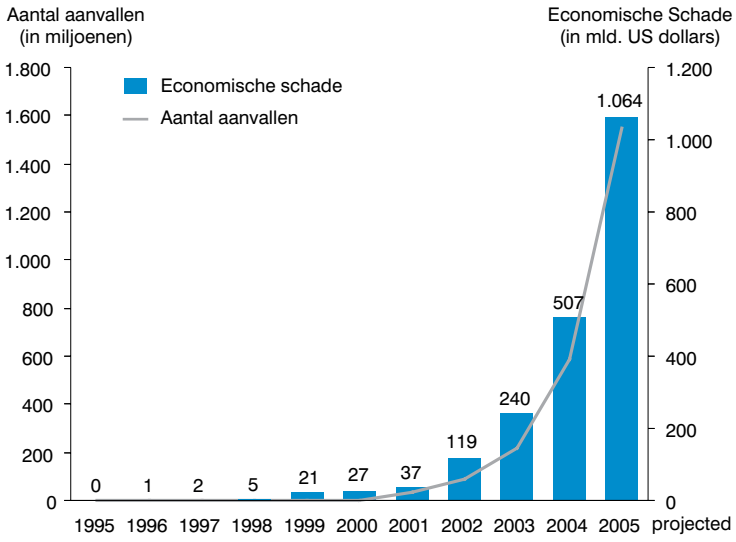
Figuur 18: *Top-10 internetoplichting (VS, 2007)*



Bron: NCL's Fraud Center

Noot: Bij "Veilingen": Tijdens de herfst van 2003 verwijderde online gigant eBay de link op zijn website naar fraud.org. Met als resultaat dat het aantal aan NCL Fraud Center gemelde klachten nog slechts een fractie is van de aantallen voor die tijd.

Figuur 19: *De explosie van openlijke digitale aanvallen (wereldwijd)*



Bron: NCL's Fraud Center, Congressional Research Service, mi2g, Craig Fosnock, Eurobarometer e-Communications Household Survey 2007, Symantec, McAfee, Booz & Company analyse

Openlijke aanvallen zijn degene die publiekelijk bekend worden, inclusief:
- Data-aanvallen waarbij vertrouwelijkheid, authenticiteit of integriteit wordt geschonden, of
- Aanvallen waarbij controle over het netwerk of administratie-systemen in gevaar worden gebracht

generatie" op te voeden. "Born digital" zijn is geen excuus voor onrechtmatig gedrag, maar kan het wel verklaren, omdat dergelijke gebruikers gewend zijn aan het "gratis" internetmodel en verwachten zonder abonnement of betaling digitale content te kunnen downloaden.
Het internet heeft geleid tot het ontstaan van een "ondergrondse" economie voor illegale digitale activiteiten. Je kunt er bijvoorbeeld digitale producten als e-mail wachtwoorden en adressen kopen. Je kunt er ook het verzenden van spam regelen en "bots" waarmee verwoesting kan worden aangericht bij de firma's waartegen ze gericht zijn. Deze bedreigingen worden langzamerhand onderkend en er wordt op gereageerd. Zo heeft Microsoft 65 onderzoekers en advocaten in dienst die fulltime werken aan het opsporen van "cybercrime" (januari 2008).

Samenvattend kan worden gesteld dat de nu zichtbare risico's rondom de digitale wereld een zorg zijn voor zowel de consument als het bedrijfsleven; de continuïteit en groei van het internet en de digitale wereld staan op het spel.

Om de digitale wereld te laten groeien is het nodig dat de consument op de hoogte is van de gevaren en dat hij weet hoe ermee om te gaan.

2. DIGITAL CONFIDENCE: CONCEPT EN OVERZICHT

De potentiële groei van de nieuwe digitale economie wordt steeds meer beïnvloed door de mate waarin zowel traditionele als "born digital" consumenten de bedrijfstak vertrouwen inzake het leveren van veilige diensten en netwerkomgevingen, goede bedrijfsvoering en het vermogen van overheden en regelgevende autoriteiten om de consument te beschermen. Digital Confidence wordt dan ook de belangrijkste groei – of juist remmende factor – voor de digitale economie, als een maatstaf voor het vertrouwen van consumenten en leveranciers in

digitale toepassingen in de breedste zin, dat wil zeggen met een gerust hart "digitaal gaan".

De bedrijfstak is zich in toenemende mate bewust van het belang van een proactieve opstelling ten aanzien van Digital Confidence en is er, in zekere zin, mee aan de slag gegaan. Maar het is een complex probleem met vele spelers die vaak vanuit verschillende posities verschillende belangen hebben; acties worden vaak zonder overleg en samenhang gestart.

Digital Confidence is de groei- of remmende factor van de digitale economie en een maatstaf voor het vertrouwen van de consument in de digitale wereld.

Om voortgang te boeken moet de sector zich richten op de bepalende sleutelfactoren voor het oordeel van de consument over nieuwe digitale en onlinediensten en -platforms. Deze sleutelfactoren zijn afgeleid uit een analyse van het huidige Web 2.0-beleid en ontwikkelingen in wetgeving, politieke debatten, internationale (handels)akkoorden, blogging-activiteiten en media-aandacht.
De sleutelfactoren hangen samen met:

- Netwerkintegriteit en Quality of Service.
- Privacy- en databescherming.
- Bescherming van minderjarigen.
- Preventie illegaal kopiëren en diefstal.

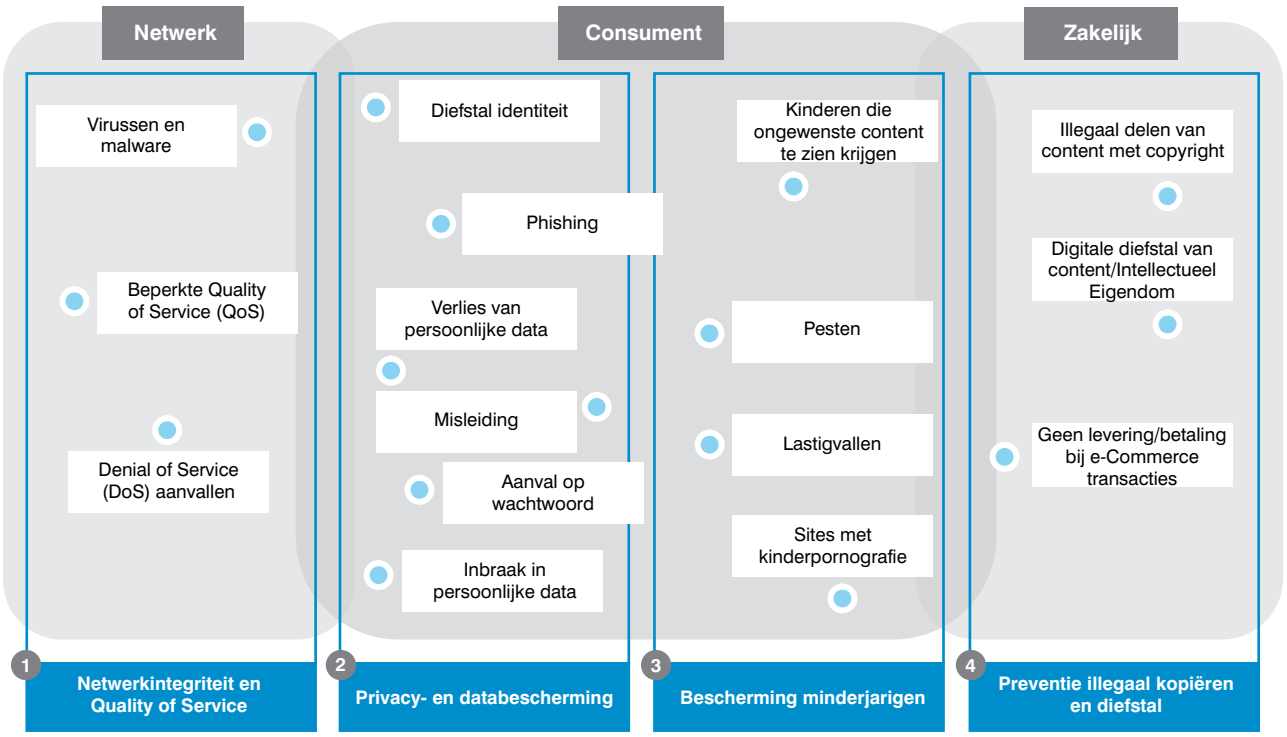
De bedrijfstak moet proactief handelen door deze zaken op een holistische manier te beschouwen, zoals in dit document is gevat in het concept "Digital Confidence". Digital Confidence gaat verder dan corporate verantwoordelijkheid en naleving van regels – het wordt al een commerciële noodzaak en een voorwaarde om te kunnen werken. Zoals bepaalde voorbeelden zullen aantonen, betekent louter naleving van regels geen consumentenacceptatie.

De vier pijlers onder het concept Digital Confidence zijn gevat in een raamwerk (figuur 20) en dekken de belangrijkste bedreigingen, onderwerpen en aanvallen die op dit moment van belang zijn voor de consument. Het raamwerk structureert en identificeert per pijler de risico's waarmee moet worden afgerekend:

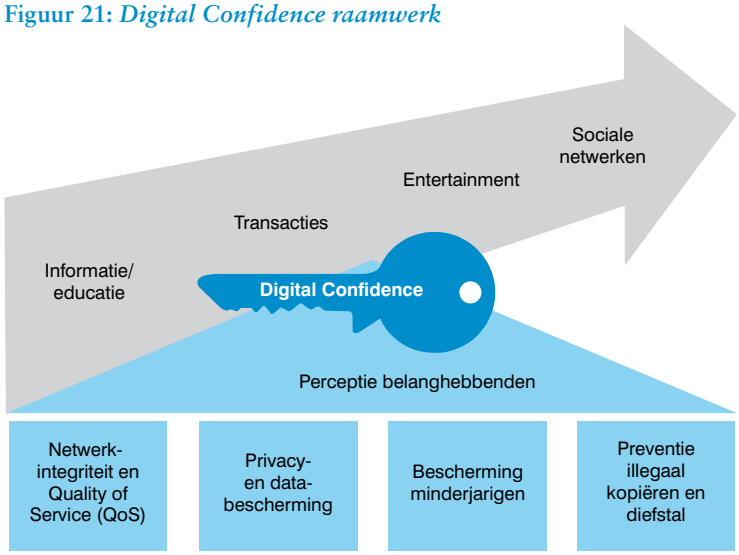
- **Netwerkintegriteit en Quality of Service.**
Hoe handhaven we netwerkintegriteit onder externe IT-aanvallen? Hoe organiseren we netwerkmanagement zo dat de gebruikerservaring optimaal is?

Zorgen voor een eerlijke verdeling van netwerkbandbreedte tijdens piekuren, op de juiste manier omgaan met toenemend dataverkeer en bescherming bieden tegen malware.

Figuur 20: *De vier pijlers van Digital Confidence*



Figuur 21: *Digital Confidence raamwerk*



- **Privacy- en databescherming.** Hoe beschermen we de privacy en data van de consument online? Voorkomen van identiteitsdiefstal, verlies van persoonsgegevens en commerciële exploitatie.

- **Bescherming van minderjarigen.** Hoe te zorgen voor de veiligheid van kinderen online? Bescherming tegen ongewenste sites, pesten en grooming, bestrijden van kinderpornografie.

- **Preventie illegaal kopiëren en diefstal.** Hoe om te gaan met inbreuk op copyright? Bestrijden van diefstal van auteursrechtelijk beschermd materiaal, beschermen van e-commerce-transacties.

Binnen deze vier pijlers beïnvloeden een aantal verschillende belanghebbenden het niveau van Digital Confidence, of worden erdoor beïnvloed.

Dit rapport brengt onderzoeken over Digital Confidence onder de aandacht die laten zien wat de beste aanpak is en wat er noodzakelijk is om door de bedrijfstak proactief opgezette initiatieven in een stroomversnelling te brengen. Het doel is bij te dragen aan het denken over gepaste en in de juiste mate gedoseerde interventieniveaus en samenwerkingsvormen tussen bedrijfstak en overheden; Digital Confidence laten opbloeien met inachtneming van fundamentele internetvrijheid en vereisten vanuit het zakenleven.

*Sociale netwerken maken pesten via het internet mogelijk – 70 procent toename van pesten bij minderjarigen die sociale netwerken gebruiken.**

**Bron: Pew Internet & American Life Project*

2) Bij een Denial of Service (DoS) aanval zenden veel machines data naar één doelmachine. De consequentie hiervan is dat de doelmachine wordt overladen met data, waardoor het systeem crasht of op z'n minst onbruikbaar wordt

3. NETWERKINTEGRITEIT EN QUALITY OF SERVICE

Netwerkintegriteit en Quality of Service richten zich op het mogelijk maken en beveiligen van technologieplatforms voor de digitale wereld. Er zijn twee hoofddoelstellingen:

1. Zorgen dat het netwerkplatform en de computeromgeving van consumenten en bedrijven veilig en beschermd zijn tegen externe aanvallen – consumenten en bedrijven mogen geen last hebben van vijandige digitale aanvallen zoals virussen, malware – zoals spyware – en Trojaanse paarden die informatie verzamelen of vernietigen, plus een stroom spam van websites waardoor Denial of Service kan optreden.[2)]

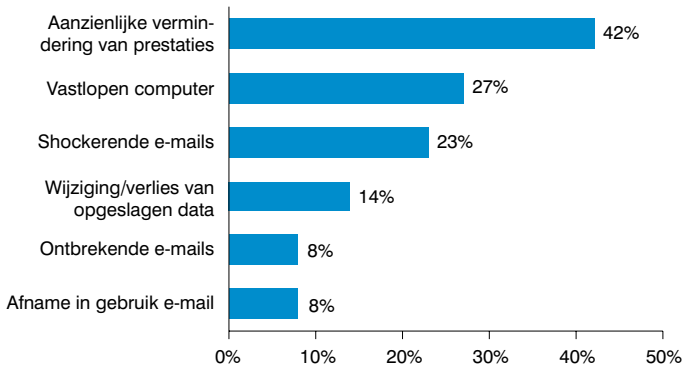
2. Zorgen dat eindgebruikers verzekerd zijn van een constante Quality of Service – het netwerk kan het toenemende gebruik aan, zodat bij de eindgebruiker de Quality of Service ondanks pieken in het netwerkgebruik constant blijft.

VIRUSSEN EN MALWARE

Virussen en malware zijn vijandige aanvallen op computers van eindgebruikers en lokale netwerken die leiden tot uiteenlopende problemen (figuur 22). Hoe bewust men zich is van de problemen rond spam en virussen hangt samen met de intensiteit waarmee het internet gebruikt wordt. In landen die een intensief gebruik kennen is men zich beter bewust van de gevaren en worden beveiligingsmaatregelen beter op waarde geschat. In de Scandinavische landen en de Benelux is men zich bijvoorbeeld goed bewust van de gevaren van vijandige digitale aanvallen: meer dan 35 procent denkt het slachtoffer te zijn (geweest) van spam en virussen. In de zuidelijke Europese landen daarentegen

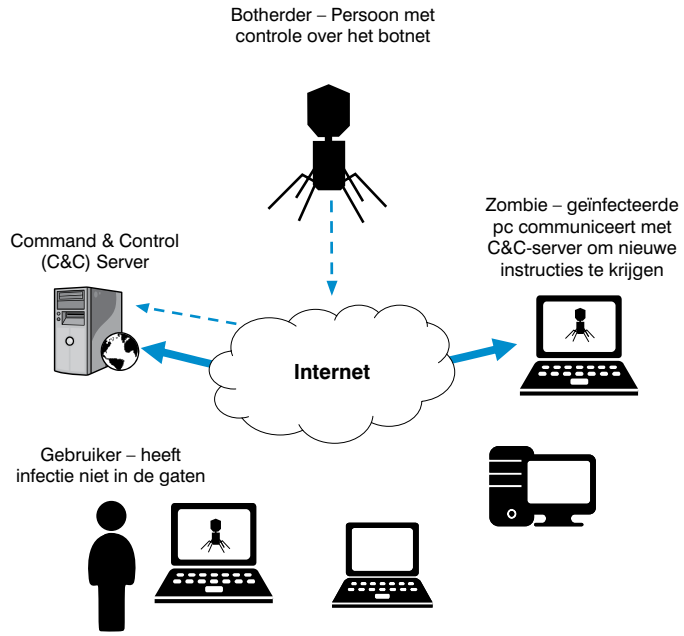
Spam vermindert het vertrouwen van consumenten in e-mail en 18 procent ziet het als een groot probleem

Figuur 22: *Problemen voortkomend uit spam en virussen (VK, 2007)*



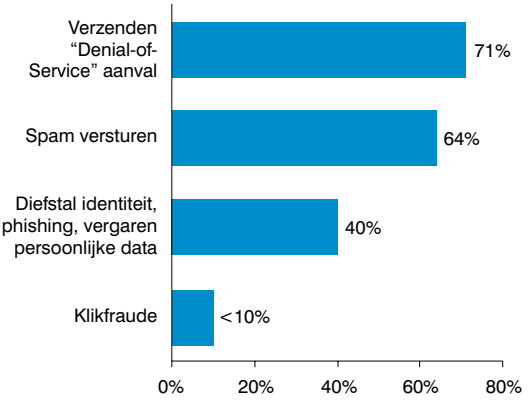
Bron: Eurobarometer e-Communications Household Survey Huishouden Research 2007

Figuur 23: *Botnets – de "Botherder" en zijn zombies*



Bron: WatchGuard

Figuur 24: *Gebruik van botnets voor aanvallen*



Bron: Arbor

heeft slechts 15 procent last. In de Verenigde Staten is door spam bij 55 procent het vertrouwen in e-mail afgenomen; 18 procent ziet spam als een "groot probleem".

Het meest algemene gevolg van spam, virussen en spyware is schade aan de hardware. De Consumers Union heeft uitgezocht dat spam er in een periode van zes maanden toe heeft geleid dat bijna een miljoen Amerikaanse huishoudens een nieuwe computer moest aanschaffen.

Zogenaamde botnets zijn wereldwijd verantwoordelijk voor 80 procent van de spam.

Bij de consument is er sprake van een toenemend bewustzijn van deze risico's en het is duidelijk dat men steeds meer bereid is verantwoordelijkheid te nemen voor de bescherming van de eigen hardware. Wereldwijd zet de softwarebeveiligingssector jaarlijks $9,1 miljard om en dit neemt jaarlijks met 12 procent toe.

BOTS, ZOMBIES EN BOTNETS

Een bot is software die op een semi-intelligente manier automatisch taken uitvoert.[3)] Bots kunnen door een aanvaller (botherder) gebruikt worden om op afstand computers aan te vallen; dit worden dan zgn. zombiecomputers (figuur 23). De aanvaller kan dan op de zombiecomputer bijna alle gewenste taken uitvoeren.

Botnets worden gebruikt voor diverse doeleinden, variërend van spam en Denial of Service (DoS) tot phishing en klikfraude (een aanval op advertentieproviders: de bot suggereert duizenden bezoekers op de advertentie per uur) en identiteitsdiefstal (figuur 24).

De gecombineerde bandbreedte van enige duizenden pc's, de meeste met breedbandverbinding, kunnen ernstige DoS-aanvallen veroorzaken en zijn verantwoordelijk voor 80 procent van de spam wereldwijd.

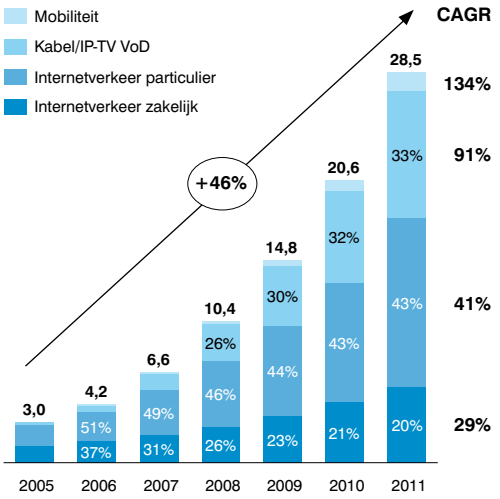
Een botnet beschrijft alle zombies die onder de controle van één botherder staan. Bekende voorbeelden van botnets:

- **Kraken.** bijna 500.000 zombies, waaronder pc's bij 50 Fortune 500-bedrijven, nagenoeg onvindbaar voor antivirussoftware.
- **Srizbi.** meer dan 300.000 zombies.
- **Storm.** Circa 150.000 tot 200.000 zombies.
- **Bobax.** Een mogelijke voorganger van Kraken of een aparte botnet.

Niet alleen zakelijke gebruikers of consumenten worden het slachtoffer van botnets. Zelfs landen kunnen het slachtoffer worden van Denial of Service-aanvallen. In 2007 zijn in Estland het parlement, de meeste ministeries, politieke partijen, drie van de zes grote nieuwsagentschappen, twee van de grootste banken en communicatiebedrijven het slachtoffer geworden van Denial of Service-aanvallen.

3) Bots zijn stukjes software op een lokaal systeem en ontvangen taken van een server op afstand. De bot voert zo autonoom mogelijk taken uit en wacht dan op nieuwe opdrachten

Figuur 25: *Groei IP-verkeer wereldwijd (2005–2011 in ExaBytes per maand)*



Bron: Cisco

QUALITY OF SERVICE

Voor zover Quality of Service-problemen aan het netwerk te wijten zijn (Quality of Service hangt af van het "end-to-end-path" over het gehele internet, niet alleen van het toegangsnetwerk) zijn er twee hoofdoorzaken aan te wijzen: het toenemende internetverkeer en de pieken in het verkeer die veroorzaakt worden door zware gebruikers met tegelijkertijd bandbreedte-intensieve toepassingen gebruiken.

Voorlichting van minderjarigen en netwerkintegriteit

Frankrijk, mei 2008: de autoriteiten arresteren 22 mensen op verdenking van hacken in een internationale hackersgroep. Verontrustend is dat 16 van de 22 verdachten jonger zijn dan 18 jaar.

Beveiligingexperts van Sophos zijn blij met dit succes, maar vragen "wat er tijdens de scholing fout gaat dat jongeren het hacken van computers aanvaardbaar vinden. Er moet op scholen meer aandacht komen voor het verantwoordelijk omgaan met computers."

De laatste jaren is het internetverkeer sterk gegroeid en deze groei zal zich ook in de toekomst voortzetten (figuur 25). Er zijn maatregelen nodig om de verwachte groei door toepassingen als video-on-demand, HDTV, filesharing, user-generated video, P2P en online gokken op te vangen. Dit type toepassingen zal voor de volgende groeifase in de digitale wereld zorgen. Dit rapport behandelt alleen QoS voor zover het aan IP-services gerelateerd is. Kabelexploitanten zorgen voor QoS door het gebruik van "dedicated spectrum"; dit heeft geen invloed op de breedbandsnelheid. Anders is het in een IP-omgeving, waar (meerdere) IPTV-streams een aanslag doen op de breedbandcapaciteit.

Het tweede zorgpunt heeft te maken met de "zware gebruiker". Breedbandnetwerken zijn – zoals alle netwerken – ontworpen om piekbelastingen zoals die optreden gedurende de drukste perioden voor netwerkverkeer, aan te kunnen. Door "grootgebruikers" wordt de in het ontwerp ingebouwde maximumcapaciteit overschreden. Zonder actief netwerkmanagement krijgen eindgebruikers te maken met afnemende Quality of Service. Deze afname kan verschillen en hangt af van de toepassing (bijvoorbeeld internetbankieren versus mp3-downloads). In breedbandnetwerken, waar capaciteit door iedereen gedeeld wordt, leidt dit tot afnemende snelheid in verbindingen of, in extreme gevallen, tot uitval.

Zware gebruikers doen een aanslag op de Quality of Service voor alle gebruikers.

Om het overschrijden van de netwerkcapaciteit te voorkomen, kunnen operators de capaciteit verhogen (nieuwe infrastructuur aanleggen of de bestaande upgraden), wat extra kosten met zich meebrengt. Ook kunnen ze actieve technieken voor dataverkeermanagement toepassen waardoor bandbreedte beschikbaar blijft voor bepaalde soorten gebruik voor alle gebruikers.

Zuiver geredeneerd vanuit de beschikbare capaciteit is het toevoegen van extra capaciteit de meest voor de hand liggende oplossing, maar dit heeft een belangrijk economisch gevolg. Door de snelle groei van het dataverkeer zullen netwerkproviders meer en meer capaciteit moeten toevoegen en daardoor gaan de netwerkkosten omhoog. Die kosten moeten worden opgebracht door de consumenten die gebruikmaken van het netwerk, waardoor de prijzen voor de eindgebruiker stijgen. Alleen meer capaciteit toevoegen zal de problemen rond netwerkcongestie en afnemende Quality of Service tijdens piekuren niet oplossen. Afhankelijk van het type internettoepassing, netwerkdimensies en de snelheid van de bronapparatuur, zal tijdens piekbelasting waarschijnlijk altijd de maximaal beschikbare bandbreedte worden gebruikt, ongeacht alle door de provider uitgevoerde capaciteit upgrades.

Om de verstopping die door toepassingen met een groot gebruik van bandbreedte worden veroorzaakt te verminderen, gebruiken operators technieken voor actief dataverkeermanagement. Naast technische oplossingen worden prijsstellingen op basis van gebruik overwogen. Dit stimuleert consumenten om drukke tijden te vermijden en op andere tijden online te gaan.

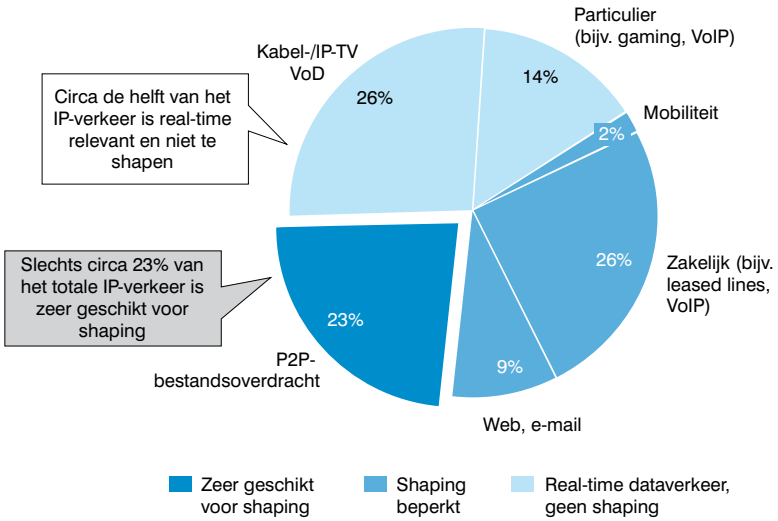
Technisch actief dataverkeermanagement wordt vaak bandbreedtemanagement of "data-verkeer-shaping" genoemd. Deze technieken herkennen verkeer dat geen hoge priorteit heeft of niet realtime is en kennen er op het netwerk een lagere prioriteit aan toe. Als een gevolg van bandbreedtemanagement kunnen niet-realtime datadownloads, zoals het downloaden van muziek van iTunes, wat langer duren. Daarentegen kan er ongehinderd gebruikgemaakt worden van tijdgevoelige toepassingen als streaming muziek of VolP-telefonie.

Dataverkeermanagement biedt slechts een deel van de oplossing om optimaal internetverkeer over breedbandnetwerken mogelijk te maken. Dataverkeermanagement gebaseerd op shaping, waarvan de eindgebruiker geen last ondervindt, kan alleen worden toegepast op niet-realtime verkeer en dat betreft slechts een kwart tot de helft van het totale IP-verkeer (figuur 26).

De bedrijfstak onderkent sinds enige tijd dat een klein deel van de gebruikers een onevenredig deel van het internetverkeer voor z'n rekening neemt. Bij veel netwerkproviders wordt 80 procent van de bandbreedte gebruikt door minder dan 10 procent van de gebruikers. Dit is niet alleen een voorbeeld van een oneerlijke gebruiksverdeling, het verergert ook de bandbreedteproblemen bij de piekbelastingen. Het grootgebruik hangt samen met peer-to-peer- en videotoepassingen; netwerkoperators maken zich grote zorgen over de gevolgen van deze populaire toepassingen voor verstoppingen in het internetverkeer. Zo leidde de introductie door de BBC van de iPlayer direct tot een toename in bandbreedtegebruik als gevolg van videostreaming.

De situatie in Groot-Brittannië rond het BBC iPlayer-platform is een typisch voorbeeld van de dilemma's waar de industrie mee wordt geconfronteerd. De iPlayer wordt gebruikt om radio- en videosignalen te verspreiden en bekijken via het internet. In de eerste drie maanden na de introductie van de iPlayer in december 2007 zijn er meer dan 42 miljoen programma's gestreamd of gedownload. Er is in Groot-Brittannië een verhit debat ontstaan tussen de platformoperator BBC, diverse internetproviders en regelgevende instanties over het ongekend intensieve gebruik van het platform. Veel ISP's die zich zorgen maken over de bandbreedtevereisten hebben de BBC verzocht mee te betalen aan de noodzakelijke netwerkupgrades. De BBC heeft deze claims als onaanvaardbaar verworpen en heeft de ISP's gewaarschuwd dat als operators de inhoud veranderen door "squeezing, shaping of capping" de BBC op het platform aan zal geven bij welke ISP's de inhoud het best tot zijn recht

Figuur 26: ***Toepasbaarheid shaping van dataverkeer: verdeling van wereldwijd IP-dataverkeer 2008***



Bron: Cisco, Booz & Company analysis

komt en welke ISP's je het best kunt vermijden. Ofcom heeft een schatting gemaakt van de kosten om het door iPlayer met 3GB per maand per gebruiker gestegen gebruik te faciliteren. De netwerkproviders in Groot-Brittannië zouden in de komende vijf jaar tot £831 miljoen moeten opbrengen om hun netwerken te upgraden. Voor de ISP's is het de vraag wie er moet gaan betalen voor de benodigde extra capaciteit; de platformprovider of de consument. Als reactie hierop stelde Ofcom in april 2008 haar positie vast: "investeringen moeten worden opgebracht door netwerkoperators en consumenten samen, de prijzen voor snellere verbindingen zullen waarschijnlijk stijgen" *. Ofcom beveelt "content-controlled tariff models" aan waarbij ISP's en de contentproviders samen diensten aanbieden op gegarandeerd soepele netwerken, maar wel tegen een bij het product passende consumentenprijs.

Minder den 10 procent van de gebruikers is goed voor meer dan 80 procent van het netwerkverkeer.

Het managen van de capaciteit en het gebruik van netwerken heeft duidelijk voordelen voor het grootste deel van de eindgebruikers: zij kunnen er zeker van zijn dat de Quality of Service aan hun verwachtingen blijft voldoen.

Dit heeft evenwel z'n prijs; met de toename van dataverkeer door veel bandbreedte gebruikende toepassingen, zoals video-on-demand, zijn extra investeringen nodig. Deze moeten mede worden opgebracht door hogere prijzen, meer producten met gefaseerde toegankelijkheid, of duidelijk gedifferentieerde manieren om internetverkeer gedurende drukke perioden te beheren.

Het managen van dataverkeer tijdens piekuren is een effectieve manier om de Quality of Service voor verreweg het grootste deel van de gebruikers veilig te stellen.

** Ofcom CEO Ed Richards*

In feite wordt met technieken voor dataverkeermanagement gezocht naar een evenwicht tussen Quality of Service, de kosten voor het aanleggen van netwerken en stijgende prijzen voor de eindgebruiker.

Migratie van de huidige breedbandnetwerken naar Next Generation-netwerken (NGN) met een aanzienlijk grotere capaciteit zal voor een deel de groeiende vraag naar bandbreedte voor tijdgevoelige toepassingen en diensten kunnen opvangen. Maar dit betekent niet dat dataverkeermanagement voor niet-realtime diensten onbelangrijk gaat worden.

ACTIEF DATAVERKEERMANAGEMENT: OVERZICHT

Er bestaan verschillende technische mechanismen die netwerkoperators kunnen gebruiken om actief dataverkeer op hun netwerk te beheren en zo de beschikbare bandbreedte te optimaliseren. Ze zijn allemaal gebaseerd op het besparen van bandbreedte die door specifieke datastromen wordt gebruikt gedurende piekuren en door grootverbruik. De methodes zijn tweeledig: (i) identificeren van het dataverkeer die geshaped moet worden en (ii) dit deel van het dataverkeer een lagere prioriteit toekennen waardoor de bandbreedte die door dit dataverkeer gebruikt wordt gereduceerd wordt.

DATAVERKEER-IDENTIFICATIE EN SELECTIE

Of dataverkeer geshaped kan worden, kan op diverse manieren in kaart worden gebracht (figuur 28). Een simpele manier is alleen gericht op de bron of op de target IP-adressen en -poorten (bijvoorbeeld om een redelijk gebruik van bandbreedte af te dwingen).

Dataverkeer in kaart brengen op basis van IP-adressen en -poorten is niet erg nauwkeurig. Hierbij worden alleen grote “brokken” dataverkeer geselecteerd, wat effect kan hebben op een groot aantal toepassingen (bijvoorbeeld als een poort gebruikt wordt door meerdere systemen.

Een alternatieve en geavanceerdere methode is het bepalen of dataverkeer geschikt is voor shaping middels deep packet inspection (DPI). Elk IP-pakket krijgt een profiel toegewezen, zodat het onderliggende protocol wordt gelezen en voorzien van een handtekening. Deze handtekening kan worden vergeleken met een lijst bekende handtekeningen. Aan de hand hiervan kan het pakket geclassificeerd worden, bijvoorbeeld als video-on-demand. Uitgaande van deze identificatie kunnen specifieke protocollen of zelfs diensten geselecteerd of gedeselecteerd worden voor shaping (bijvoorbeeld realtime toepassingen). Cruciaal voor DPI is dat de handtekeningendatabase frequent wordt onderhouden en geactualiseerd als antwoord op de snel veranderende internetarchitectuur.

Het grootste nadeel van DPI zijn de kosten: omdat elk afzonderlijk pakket moet worden geïnspecteerd, is veel apparatuur nodig. Systemen gebruiken meestal een gemengde aanpak: dataverkeer wordt van tevoren gefilterd op basis van IP-adres en poort, DPI wordt alleen toegepast op de geselecteerde pakketten.

Samenvattend kan het selecteren van dataverkeer gebruikersspecifiek (op basis van IP-adres), protocolspecifiek (op basis van

BBC iPlayer: casestudie

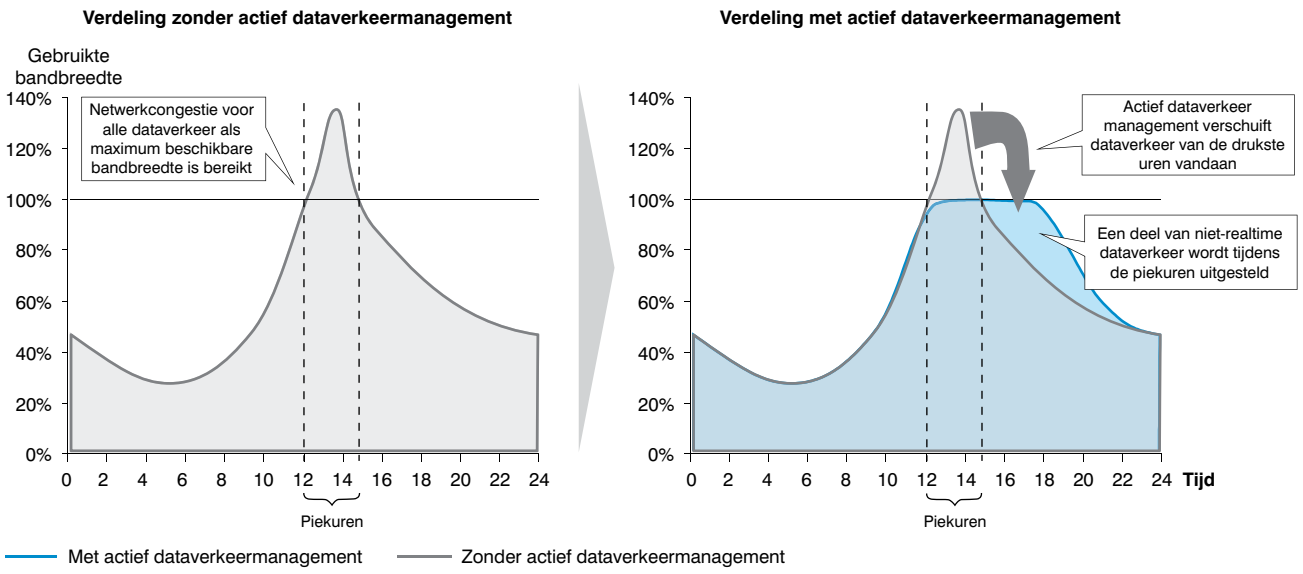
Volgens gegevens uit februari 2008 van de Britse ISP Plusnet, is het internetverkeer sinds de introductie van iPlayer aanzienlijk toegenomen:

- Het per gebruiker streamen van video’s nam van 180 MB in december toe naar 292 MB in januari... een stijging van 62 procent.
- Het aantal streams overtreft het aantal downloads achtvoudig.
- De kosten voor streaming dataverkeer zijn in dezelfde periode verdrievoudigd.

Bovenstaande toont een trend waarbij gebruikers als zij kunnen kiezen tussen stream en download, liever streamen dan wachten op een volledige download. Waarschijnlijk bestaat er een verschil tussen het gebruik van muziek en dat van video’s. Consumenten zullen muziek vaker willen gebruiken en downloaden, terwijl video’s als stream bekeken worden.

Als dit inderdaad een trend is zal dataverkeermanagement, omdat het niet toe te passen is bij tijdgevoelige streams, minder effectief zijn. De focus komt dan weer op het uitbreiden van capaciteit te liggen.

Figuur 27: *Management van dataverkeer*



Bron: Booz & Company

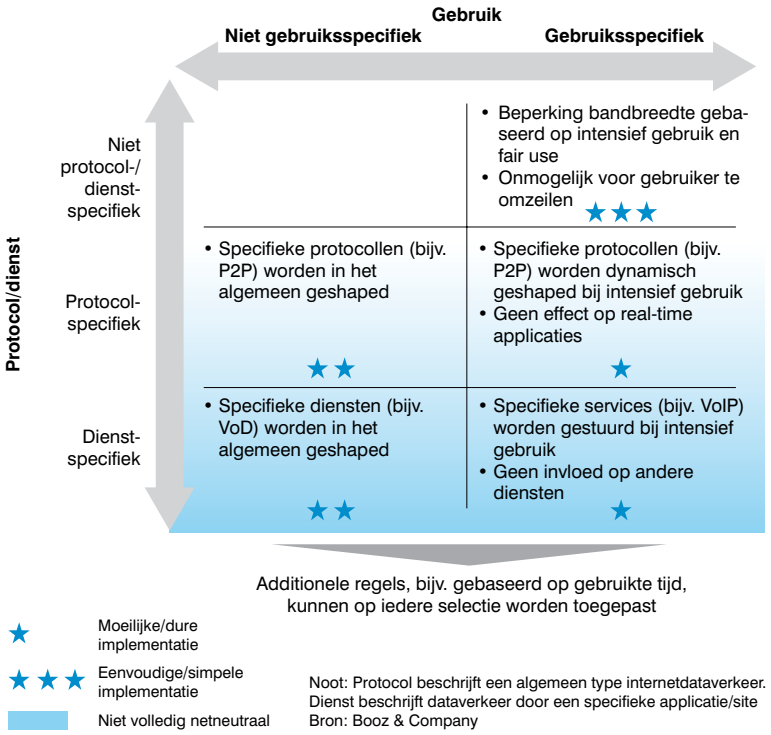
poortselectie of DPI; bijvoorbeeld mailprotocol) en/of servicespecifiek (waar een service een bepaalde server of toepassing is, bijvoorbeeld YouTube of BitTorrent) plaatsvinden.

PRIORITEITEN STELLEN VAN DATAVERKEER

Er bestaan diverse methodes om de prioriteit, en daarmee de gebruikte bandbreedte door specifieke datastromen, te verhogen of verlagen. Sommige van deze methodes kunnen in ieder IP-netwerk worden gebruikt, terwijl andere speciaal voor specifieke netwerken zijn ontworpen. Zo is PCMM (packet cable multi media) een QoS-oplossing speciaal gecreëerd voor kabelnetwerken.

Alle technieken vertragen geselecteerde delen dataverkeer en verminderen daarmee de datastroom op het netwerk. Voor de eindgebruiker betekent het toepassen van dataverkeermanagement dat het bij niet-realtime dataverkeer lange downloads kan vertragen, maar het heeft geen invloed op e-mail of op het browsen.

Figuur 28: *Dataverkeer selectie*



Noot: Protocol beschrijft een algemeen type internetdataverkeer. Dienst beschrijft dataverkeer door een specifieke applicatie/site
Bron: Booz & Company

4. PRIVACY- EN DATABESCHERMING

Privacy- en Databescherming betreft de veiligheid van digitale data van individuen. Het dient vier hoofddoelen:

1. Beschermen van de persoonsgegevens van consumenten tegen publicatie, ongewild of door henzelf (bijvoorbeeld door websites voor sociaal netwerken), doordat de database van de operator wordt gehackt, of door het onzorgvuldig, onveilig verzenden van data.

2. Voorkomen dat persoonsgegevens van consumenten commercieel worden gebruikt, bijvoorbeeld ter ondersteuning van advertentiecampagnes, zonder dat de betrokken individuen het weten. Voorbeeld: bedrijven kunnen gegevens over burgerlijke staat en familieomstandigheden van individuen gebruiken voor gericht online adverteren.

3. Beschermen van persoonsgegevens van de consument tegen illegale toegang, bijvoorbeeld door misleiding of phishing.

*De gemiddelde persoon heeft 36 GB data opgeslagen bij instanties; dit is het equivalent van 80 uur video of één miljoen pagina's tekst.**

4. Voorkomen van diefstal van en fraude met identiteit; criminelen stelen geld of verrijken zich op een andere manier door persoonsgegevens van een ander individu te kopiëren en te gebruiken.

Bij Privacy- en Databescherming staan twee methodes centraal: ten eerste ongewilde of opzettelijke publicatie en ten tweede op illegale wijze verkregen data, bijvoorbeeld door phishing.

DATAPUBLICATIE

Er is een toenemend aantal websites voor sociaal netwerken op het internet. Van websites met een speciale doelgroep (bijvoorbeeld Facebook) tot websites die zich richten op professioneler netwerken (bijvoorbeeld Linkedin). Deze websites vragen, publiceren en bezitten groeiende hoeveelheden informatie over gebruikers, inclusief woonplaats, leeftijd, interesses en foto's. De meeste websites bieden de mogelijkheid tot beperkte toegang tot deze gedetailleerde persoonsprofielen, maar bijna de helft van de gebruikers maakt zijn of haar profiel toegankelijk voor iedereen. Ook veel andere websites verlangen van gebruikers dat zij zich registreren om de site te gebruiken (bijvoorbeeld webmailproviders) of om alle mogelijkheden te gebruiken en alle pagina's te bezoeken (bijvoorbeeld veel forumsystemen). Deze sites verzamelen ook gegevens over (het gedrag van) de gebruikers.

Het openbaar beschikbaar stellen van dit soort informatie heeft implicaties voor de persoonlijke veiligheid, beveiliging en reputatie.

Second Life – het gevaar van op de verkeerde plaats terechtkomen

Een Duitse moeder rapporteerde in 2008 dat haar dertien jaar oude dochter helemaal opging in Second Life, een virtueel platform dat gebruikers een "identiteit" en een "leven" in een virtuele wereld biedt.

De dochter vroeg haar moeder geld om Linden-dollars, het geld in Second Life, te kunnen kopen. De moeder weigerde.

Maanden later ontdekte de moeder dat haar dochter, om aan Linden-dollars te komen, virtueel was gaan strippen en zich prostitueerde in een club in Second Life.

Zo bestaat het gevaar van identiteitsdiefstal, of als bedrijven persoonlijke informatie van websites voor sociaal netwerken gebruiken om sollicitatiegegevens te controleren, of gebruiken bij het zoeken naar geschikte kandidaten op sites van professionele organisaties. Bovendien kan informatie niet meer worden teruggetrokken omdat in de digitale wereld van het internet alles heel makkelijk te kopiëren, te verspreiden en te bewaren is.

Missouri/de Verenigde Staten, mei 2008: Cyberpesten illegaal na zelfmoord

Na de zelfmoord van een dertien jaar oud meisje dat via het internet gepest werd door de buren, is er een wetsvoorstel gedaan om cyberpesten illegaal te maken. Lastigvallen en intimideren kan bestraft worden met maximaal twee jaar gevangenisstraf.

Eerste reacties zijn dat het moeilijk is om onderscheid te maken tussen "normale" grappen tussen vrienden en lastigvallen. Ook zal het moeilijk zijn de wet te handhaven.

Niet alleen de consumenten zelf, maar ook bedrijven zijn een bron van gevaar voor privacy. Digitaal opgeslagen informatie is voor organisaties gemakkelijk te managen, te gebruiken en te delen. Tegelijkertijd is de kans op het onbedoeld publiek toegankelijk maken van informatie groter, zoals geïllustreerd wordt door een recente zaak in Groot-Brittannië. Het Britse departement van Revenue and Customs heeft zijn excuses moeten aanbieden aan de klanten van de Investeringsbank UBS Laing and Cruickshank nadat zij gevoelige accountinformatie was kwijtgeraakt. Het departement verloor een computerschijf die het van de bank had ontvangen met adressen en accountdetails van investeerders in USB's Personal Equity Plan. Het was de fout van een individu, maar laat zien hoe concreet en hoe groot het risico is.

*Internetgebruikers worden zich meer bewust van hun digitale voetafdruk – 47 procent zoekt online informatie over zichzelf. Maar 60 procent is niet bezorgd over de hoeveelheid informatie die online gevonden kan worden.***

Bedrijven gebruiken de gedetailleerde consumenteninformatie in hun bezit ter ondersteuning van legale transacties. Zo verkopen "super servers" als

*De CIA gebruikt Facebook bij het rekruteren van nieuwe werknemers.****

* Bron: IDC

** Bron: Pew Internet & American Life Project

*** Bron: Wired, 2007

Meredith, een Amerikaans mediabedrijf, uittreksels van hun database. Deze database bevat informatie over 85 miljoen Amerikaanse burgers, inclusief details over zes van iedere tien vrouwen en acht van iedere tien huishoudens. Meredith heeft ondernemingen in digitaal adverteren opgenomen in het bedrijf om de waarde van de informatie door gerichte advertenties te gelde te maken.

PHISHING

Phishing is de meest gebruikte methode om onrechtmatig persoonsgegevens te verkrijgen. Men vermomt zich als betrouwbare entiteit om gevoelige informatie binnen te halen, zoals gebruikersnamen, wachtwoorden en creditcardgegevens. Deze aanvallen zijn gericht op eindgebruikers, waarbij het grootste deel (meer dan 65 procent) zich voordoet als e-commerce-site, eBay of PayPal.

Phishing baart de bedrijfstak steeds meer zorgen: elke succesvolle aanval resulteert in een verlies van gemiddeld $220 per individuele consument. En het probleem wordt steeds groter – in 2007 werden elke maand 30.000 nieuw phishing-sites in kaart gebracht.

Zorgen voor bescherming van privacy en gegevens wordt steeds moeilijker door de diversiteit van bedrijven die informatie van mensen in digitale vorm in bezit hebben – van zakelijke organisaties (retail, banken) tot overheidsinstanties en sociale netwerken.

Phishing-aanvallen zijn de meest gebruikte methode om privégegevens te verkrijgen – en 65 procent ervan doet zich voor als belangrijke e-commerce-site.

Verder is de definitie van persoonsgegevens een dynamische kwestie die in het licht van de technologische vooruitgang herzien moet worden (of een IP-adres bijvoorbeeld al dan niet persoonlijke informatie is wordt hevig betwist). Daarnaast is het belangrijk hoe toestemming moet worden verleend om gegevens te mogen delen. Twee modellen staan ter discussie: "opt-in" versus "opt-out" – de eerste variant vereist dat consumenten er actief mee instemmen dat hun gegevens worden gedeeld. De tweede is minder populair, omdat deze toestaat dat gegevens standaard worden gedeeld, tenzij de consument het verbiedt. En het is niet altijd duidelijk of en hoe ze dat moeten doen. Meer transparantie over het gebruik van persoonlijke gegevens zal veel zorgen wegnemen rond de discussie over opt-in versus opt-out.

Duidelijk is dat het verzamelen van illegale gegevens een criminele handeling is. Maar gezien het internationale karakter ervan is bestraffing moeilijk. De meeste phishing-aanvallen komen van criminelen in een ander land dan de slachtoffers, met apparatuur die zich vaak in een derde land bevindt dat geen deugdelijke cyberwetgeving kent. Dat maakt het voor de politie bijna onmogelijk plaatselijke wetgeving toe te passen.

Phishing – uitleg en de meest gebruikte technieken

Phishing gebeurt meestal via namaak e-mails. Spamfilters zijn vaak zeer effectief, maar niet perfect.

Voorheen waren phishing-e-mails van slechte kwaliteit, slecht vormgegeven en vol spelfouten, maar tegenwoordig zijn ze sterk verbeterd – zelfs ervaren gebruikers hebben moeite het verschil te zien.

Phishing is gebaseerd op twee belangrijke technieken:

- **Linkmanipulatie.** Bijvoorbeeld "g00gle.com".
- **Websites namaken.** Phishing-sites zien eruit als de originele site, soms zelfs met adres (dankzij onvolkomenheden in de browserbeveiliging).

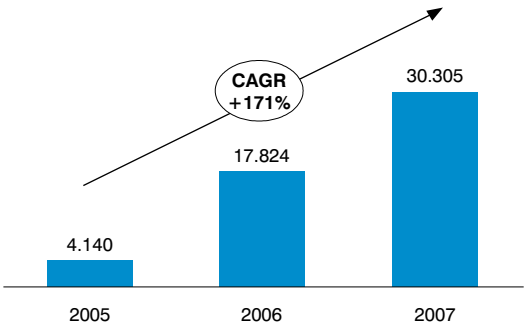
Elke maand worden meer dan 30.000 nieuwe phishing-sites in kaart gebracht – elke succesvolle aanval kost de consument gemiddeld $220.

5. BESCHERMING VAN MINDERJARIGEN

Bescherming van minderjarigen streeft ernaar het welzijn van minderjarigen in de onlinewereld te beschermen. De vier belangrijkste doelstellingen zijn:

1. Kinderen beschermen tegen het zien van ongewenste content –van seksueel expliciete tot gewelddadige en uitlokkende content waarvan ouders en de maatschappij niet willen dat kinderen de mogelijkheid hebben het te zien (bijvoorbeeld pornografie, geweld).

Figuur 29: *Gemiddeld aantal nieuwe phishing-sites (wereldwijd, per maand)*



Bron: Phishtank, APWG, NLC Fraud Center

Privacy en illegaal kopiëren

VS, mei 2008: Het Walter Reed Army-ziekenhuis maakt per ongeluk persoonlijke informatie van meer dan 1.000 patiënten openbaar. Eén bestand bevatte de gegevens en werd onbedoeld gedeeld op een peer-to-peer (P2P) syteem.

Meerdere andere data-inbreuken vonden plaats door filesharing op P2P-systemen, bijvoorbeeld bij ABN Amro en Pfizer. Hoewel het beleid van de meeste bedrijven en organisaties het gebruik van P2P-systemen verbiedt, zien sommige gebruikers het gevaar ervan niet in.

2. Pesterij voorkomen – opzettelijk vijandig gedrag gericht tegen een minderjarige door (groepen van) peers in de digitale omgeving (bijvoorbeeld "happy slapping" en het online plaatsen van vernederende persoonlijke foto's).

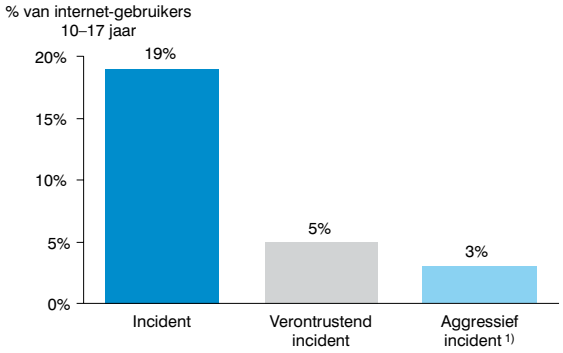
3. Voorkomen van kinderlokkerij en verleiding – waarbij volwassenen digitale omgevingen gebruiken (zoals chatrooms en sites voor sociaal netwerken) om kinderen op te sporen en een vertrouwelijke virtuele relatie met ze aan te gaan, om vervolgens persoonlijk contact te zoeken met kwade bedoelingen.

4. Het weren van kinderpornografie bij de productie van pornografisch materiaal (foto's, video's). Het gaat om drie belangrijke aandachtsgebieden: 1) vervolging van gebruikers van kinderpornografie, 2) vervolging van aanbieders van kinderpornografie en verwijderen van materiaal en 3) voorkomen dat internetgebruikers ongewild geconfronteerd worden met kinderpornografie.

Digital Confidence met betrekking tot de bescherming van minderjarigen is essentieel, omdat dit aantoonbaar het gebied is dat de meeste emoties oproept. Het is ook daadwerkelijk een bedreiging: bijna 20 procent van de jeugd heeft te maken (gehad) met online lokkerij en 25 procent krijgt ongewenst materiaal onder ogen (figuren 30 en 31). Over kinderpornografie meldde The Sydney Morning Herald in juni 2008 onthutsende getallen in samenhang met een grote golf van arrestaties van gebruikers van kinderpornografie: 99 foto's die een hacker op een "gerespecteerde Europese website" had gezet, leverden "een ongelofelijke 12 miljoen hits op in slechts 76 uur nadat op pedofielennetwerken bekend was geworden dat de plaatjes beschikbaar waren en het adres van de website bekend werd gemaakt".

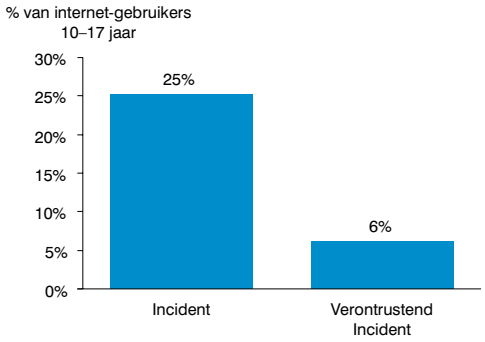
Bescherming van minderjarigen is een echt probleem; 20 procent van de jeugd in Groot-Brittannië heeft te maken (gehad) met uitlokking en 25 procent met onfatsoenlijk materiaal.

Figuur 30: *Online lastigvallen (VS, 2006)*



1) Agressief in de betekenis van lastigvallen; niet alleen online, maar ook pogingen contact met het kind op te nemen – per telefoon, post
Bron: Crimes Against Children Research Centre

Figuur 31: *Ongewenste blootstelling aan materiaal voor volwassenen (VS, 2006)*



Source: Crimes Against Children Research Centre

Toch staat de bedrijfstak voor een reeks uitdagingen. Veel ouders staan te ver af van de digitale wereld en zijn zich niet bewust van de reikwijdte van ongewenste content en het raffinement van andere kwaadwillende online praktijken, zoals grooming en pesten. Als gevolg nemen zij niet de noodzakelijke stappen om hun kinderen te beschermen bij hun online-activiteiten. Dit is met name relevant in de context van sites voor sociaal netwerken die gebruikt worden door kwaadwillende volwassenen.

*32 procent van de teenagers in de Verenigde Staten maakt mee dat persoonlijke gegevens worden doorgestuurd zonder hun toestemming.**

Er is nog een probleem bij het aangaan van de strijd met deze bedreiging: veel risico's houden nauw verband met de rijke functies van sites voor sociaal netwerken, de anonimiteit van digitale omgevingen en de mogelijkheid een valse identiteit aan te nemen. Het komt erop neer dat veel dingen die de digitale wereld verrijken ook de mogelijkheid voor ongewenste activiteiten creëren die door hun aard de duurzaamheid van de digitale wereld bedreigen.

Om deze zorgpunten aan te pakken moet de materie eerst gedefinieerd en in kaart gebracht worden. Iedereen zal het erover eens zijn dat kinderpornografie onaanvaardbaar is en alle belanghebbenden zouden moeten proberen het te voorkomen. Ook daarbuiten zal er echter nog veel discussie en meningsverschil zijn over de reikwijdte van vrijheid van meningsuiting en burgerrechten en wat (on)aanvaardbare content voor kinderen precies is en welke content als crimineel kan worden bestempeld.

6. PREVENTIE ONRECHTMATIG KOPIËREN EN DIEFSTAL

Preventie illegaal kopiëren en diefstal heeft tot doel een veilige digitale businessomgeving voor de digitale wereld te creëren. De twee belangrijkste doelen zijn:

1. Het tegengaan van het delen van auteursrechtelijk beschermde content – dat wil zeggen onrechtmatig delen van content onder auteursrecht middels toepassingen zoals peer-to-peer-netwerken.

2. Het beschermen van e-commerce-transacties – zorgen dat mensen zich houden aan de geldende servicenormen bij onlinetransacties, bijvoorbeeld bescherming tegen niet betalen, of het niet leveren van overeengekomen goederen of diensten.

Voor zakelijke en contentproviders is het essentieel om op een veilige manier te werk te kunnen gaan. Zo wordt een impuls gegeven aan de productie en beschikbaarheid van digitale en online content, wat ook de overgang naar succesvolle nieuwe, online businessmodellen zal versnellen. Diensten op het gebied van e-commerce dienen ook beschermd te worden in het geval de klant niet betaalt of de overeen-gekomen goederen of diensten niet geleverd worden. Providers van deze diensten moeten er zeker van kunnen zijn dat klanten en bedrijven zich houden aan de normen zoals die in de “offline wereld” gebruikelijk zijn bij online-transacties. De grootste zorg voor gebruikers is dat ze slachtoffer van criminele activiteiten worden, terwijl ze legitieme protocollen en toepassingen gebruiken via hun breedbandverbinding. Dit kan bijvoorbeeld het geval zijn als ze distributiesystemen gebruiken die gebaseerd zijn op P2P-technologie.

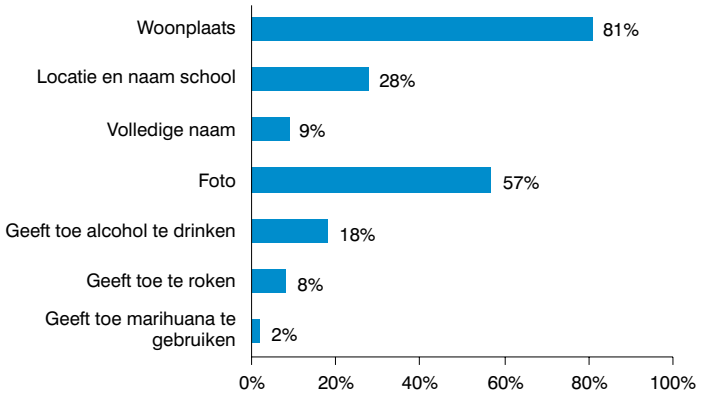
ILLEGAAL KOPIËREN: PEER-TO-PEER FILESHARING

Met de toename van beschikbare bandbreedte voor consumenten en de digitalisering van content, wordt het delen van die content erg eenvoudig. Het begon met Napster en vandaag de dag zijn er tientallen filesharing-systemen, waarvan de meeste peer-to-peer- (P2P) technologie gebruiken om de content te verspreiden. P2P-dataverkeer maakt momenteel tussen 30 en 60 procent van het totale dataverkeer uit (afhankelijk van de regio). Toen het filesharing begon, ging het voornamelijk om muziekfiles. Maar met de ontwikkeling van breedbandnetwerken werd het delen van video’s gemakkelijker en momenteel bestaat bijna 80 procent van gedeelde content uit video (figuur 34). Aangezien commerciële voorstellen van P2P-content trager op gang kwamen dan verwacht, wordt op grote schaal aangenomen dat de meeste gedeelde content tegenwoordig wordt beschermd door copyright en derhalve onrechtmatig wordt gedeeld.

Filesharing is een ware zorg voor eigenaren van content onder auteursrecht – in Duitsland is peer-to-peer-dataverkeer goed voor 50 procent van het totale netwerkverkeer.

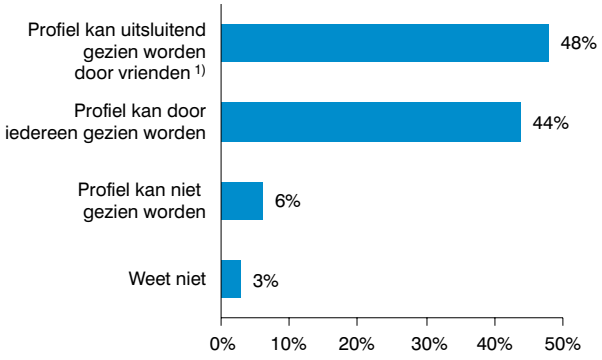
Door de exponentiële groei van IP-dataverkeer, vooral veroorzaakt door P2P-oplossingen,

Figuur 32: ***Informatie in profielen van jonge gebruikers van sociale netwerken (VK, 2007)***



Bron: Ofcom

Figuur 33: ***Zichtbaarheid van profielen in sociale netwerken (VK, 2007)***



1) Een vriend in de context van het sociale netwerk is iedereen die is toegevoegd aan een “vriendenlijst”, wat betekent dat het niet noodzakelijkerwijs een echte vriend van de persoon hoeft te zijn
Bron: Ofcom

* *Bron: Pew Internet & American Life Project*

Illegaal kopiëren en netwerkintegriteit

Begin 2007 werd een opmerkelijk en schadelijk virus gedistribueerd op het Winny-netwerk, de populairste P2P-toepassing in Japan. Het Trojaanse paard, dat de spot dreef met filesharers, dreigde hen aan te geven en zelfs te vermoorden, verwijderde een hele reeks filetypes en verving ze door plaatjes van bekende stripfiguren die waarschuwden geen P2P te gebruiken.

In Japan is het niet illegaal om virussen te schrijven, dus werd de auteur van het Trojaanse paard – een Japanse student – aangehouden wegens schending van copyright, omdat hij in zijn malware zonder toestemming afbeeldingen uit stripboeken gebruikte.

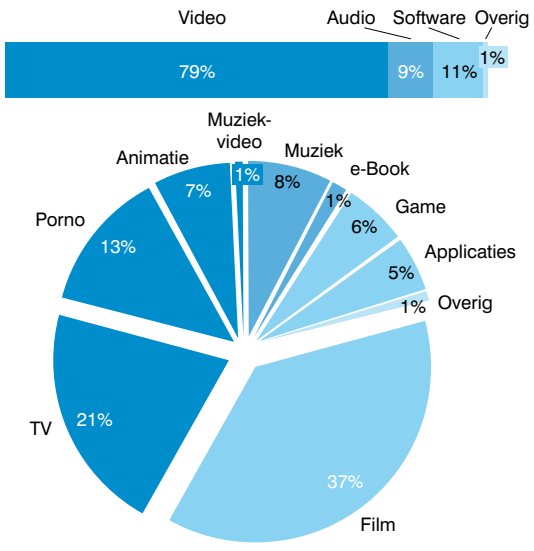
is illegaal kopiëren het meest in het oog springende probleem dat het succes van nieuwe businessmodellen bepaalt en het niveau van de ontwikkeling van online- en digitale legale contentaanbiedingen in de toekomst. Met het beschikbaar komen van breedbandproducten tot 100 Mbit/s, is de verwachting dat P2P-dataverkeer (legaal en onrechtmatig) een van de belangrijkste aandrijvers van internetverkeer blijft.

Om digitale rechten effectief te kunnen beschermen is er een reeks maatregelen geïmplementeerd door contenteigenaren, met wisselend succes en aanleiding gevend tot controverses. DRM-gebruik heeft bijvoorbeeld kritiek gekregen van politici en consumenten-groeperingen vanwege de ondoorzichtige gebruiksrechten. Dit leidde tot druk op netwerkproviders en ISP's om actiever op te treden tegen inbreuk op copyright. Netwerkproviders en ISP's worden niet verplicht om de aard van het internetgebruik van hun klanten of het dataverkeer over hun netwerken te monitoren; ten grondslag hieraan ligt het juridische principe dat hun business wordt gezien als "slechts een doorgeefluik". Toch zien we dat netwerkproviders en ISP's steeds vaker zelfregulerende codes gebruiken en bewustwordingscampagnes opzetten. Doel is bewustzijn op te wekken en een waardeperceptie te creëren rond het concept intellectuele eigendom bij de "born digital" generatie – een generatie die grotendeels van mening is dat alle digitale content gratis zou moeten zijn. Bewustmakingscampagnes en codes zijn ook onderdeel van de mitigatiemaatregelen die ter sprake komen in de context van nationale initiatieven voor (co)regulatie.

Maatregelen die in zulke gevallen overwogen worden, zijn onder meer: monitoring van dataverkeer middels DPI (deep packet inspection) en/of het filteren van de content; "Notice and Takedown" (van toepassing op netwerkproviders die content hosten); toegang beperken of blokkeren tot bepaalde sites of bepaalde protocollen; verplicht openbaar maken van persoonlijke gebruikersgegevens en IP-adressen om zo tot vervolging over te kunnen gaan; versturen van brieven naar personen als is vastgesteld dat hun internetaccount is gebruikt om onrechtmatig materiaal met copyright te delen; klanten doorverwijzen naar andere bronnen van legaal verkrijgbaar materiaal; personen die onrechtmatig blijven downloaden tijdelijk de toegang tot het internet ontzeggen – de zgn. "three strikes"-regel of "graduated response".

Al deze maatregelen roepen belangrijke vragen op over het komen tot best practices. Er moet een evenwicht worden gevonden tussen doelstellingen tegen illegaal kopiëren enerzijds en bestaande aansprakelijkheidswetgeving anderzijds (providers zijn "slechts een doorgeefluik"). Ook moeten fundamentele gebruikersrechten worden vastgesteld in relatie tot persoonlijke gegevens en onlinegedrag – ook moet rekening worden gehouden met de algemene opvattingen over een vrij internet, vrijheid van informatie en het niet digitaal uitsluiten van personen. De Europese politiek neigt ernaar de bescherming van de gebruiker voorop te stellen, met dien verstande dat hij/zij niet de bedoeling heeft winst te maken met zijn/haar actie. Downloaders afsluiten van het internet wordt gezien als een buitenproportionele maatregel tegen het licht van doelstellingen om tot een allesomvattende informatiemaatschappij te komen. Copyrighthandhaving richt zich meer op het crimineel uploaden van materiaal met copyright dan op het downloaden ervan, wat niet eens in alle jurisdicties strafbaar is. Bovendien vergen maatregelen als filtering en DPI forse investeringen van

Figuur 34: *Verdeling P2P-content, Duitsland 2007*



Bron: ipoque

BitTorrent – P2P

BitTorrent is een veelgebruikt, onvervalst P2P-protocol voor contentverspreiding. BitTorrent werkt zonder centrale fileserver: als centraal coördinatiepunt volstaat slechts een tracker-server – in wezen heeft deze twee taken: (i) torrentfiles verspreiden (indexserver, d.w.z. niet meer dan een normale file-/webserver; de torrentfile beschrijft de complete torrentdownload, en (ii) een lijst bijhouden van peers voor elke torrentfile (d.w.z. als een nieuwe node verbinding maakt geeft de tracker hem een seed-lijst van P2P-nodes om verbinding mee te maken).*

Hoewel BitTorrent ook gebruikt wordt om illegale content te verspreiden, neemt het commercieel gebruik steeds meer toe – niet-commercieel legaal gebruik zelfs nog meer. Enkele voorbeelden van BitTorrent-gebruik (volgens Wikipedia en nieuwe meldingen):

- Sub Pop Records om muziek te verspreiden, Vuze om film te verspreiden.
- Podcasting-services gebruiken BitTorrent sinds kort voor verspreiding, met name gesteund door de playersoftware "Miro".
- Amazon S3 (een opslagoplossing) gebruikt BitTorrent voor filetransfer.
- World of Warcraft gebruikt BitTorrent om updates voor de game te verspreiden (meerdere files van 100 MB).
- Verspreiding van patches; de hogeschool INHOLLAND verspreide 22 TB aan patches onder 6.500 pc's in slechts vier uur – vrijwel onmogelijk in een client/serveromgeving (het duurde vier dagen zonder BitTorrent) – en bracht het aantal downloadservers met 20 terug (voorheen 22, nu twee).

Door dit toenemend gebruik kan het protocol niet van het internet "verbannen" worden, zoals wel eens wordt voorgesteld (om filesharing te minimaliseren en ingevoerd door veel universiteiten om aansprakelijkheidsproblemen met de media-industrie te voorkomen).

* BitTorrent kan ook geïmplementeerd worden zonder een centrale trackerserver, bijvoorbeeld door verspreide "hashtables" te gebruiken (veel implementaties ondersteunen dit reeds). Dit maakt een echt P2P-systeem, zonder server, mogelijk.

Direct Download Links (DDL) – een alternatief voor P2P-filesharing

- Direct Download Links werken als normale webservers, wat betekent dat ze geen files tussen peers overbrengen.
- Gebruikers kunnen een account aanmaken en files uploaden (tot meerdere 100 megabytes). Deze files zijn te benaderen via een directe link, die alleen bij de gebruiker bekend is (dus is het doorgaans niet mogelijk om content op de DDL-server te zoeken).
- De uploader verspreidt nu de link (normaal via externe forums) en vervolgens kan iedereen de files downloaden.
- Gebruikers zonder betaalde account voor de DDL-server hebben een gelimiteerde bandbreedte en een maximum aantal downloads. Daarnaast moeten gebruikers voor elke download wachten (circa één à twee minuten voor de eerste download en langer voor volgende downloads, gebaseerd op het gebruikte volume).
- Populaire DDL-oplossingen zijn bijvoorbeeld Rapidshare en MegaUpload; momenteel zijn deze diensten niet erg populair in Europa, maar vaak gebruikt in het Midden-Oosten (9 procent van het dataverkeer daar is DDL-dataverkeer).

operators en het is de vraag wie daarvoor verantwoordelijk zou moeten zijn en voor de kosten moet opdraaien. In hoeverre waardebehoud in de contentsector gekwantificeerd kan worden en in verband kan worden gebracht met zulke maatregelen, speelt hierbij eveneens een rol. In 2007 bijvoorbeeld, suggereerde een bericht van de Value Recognition Strategy-werkgroep in Groot-Brittannië dat formatwijzigingen (d.w.z. "ontbundelen" van cd's in een "à la carte"-selectie van songs zoals bij Apple iTunes) en de prijsdruk door afgeprijsde cd's in supermarkten een grotere schadepost voor de Britse muzieksector zijn dan P2P-filesharers.

7. SAMENVATTING

Door alle vier pijlers van Digital Confidence erbij te betrekken wordt de volgende groeifase van de digitale wereld mogelijk. De acties die verschillende belanghebbenden al hebben ondernomen wijzen op een brede erkenning van de problemen en de noodzaak tot actie.

De belanghebbenden staan evenwel voor een probleem dat vele aspecten kent. Er zijn bijvoorbeeld grote verschillen in nationale wetgeving op belangrijke punten, terwijl bijvoorbeeld digitale aanvallen als phishing grensoverschrijdend zijn en internationale samenwerking voor vervolging noodzakelijk maken. Het is vaak moeilijk of zelfs onmogelijk om overtreders

De bedrijfstak ziet digital confidence als top agenda item maar heeft moeite deze effectief te adresseren.

op te sporen en te vervolgen – de maatregelen en instrumenten die voor de "analoge wereld" zijn vastgesteld voldoen simpelweg niet in de digitale omgeving. Bovendien is er een enorm grijs gebied door de snelle ontwikkeling van technologie, gedragsverandering en de nieuwe mogelijkheden in de digitale wereld; van het eenvoudig kopiëren van digitale goederen tot de wereldwijde toegankelijkheid tot het internet.

Regelgevende instanties en overheden moeten hun positie bepalen en balanceren tussen logge regelgeving, het informeren van consumenten en het handelen volgens filosofieën over de zelfregulerende markt. Cruciaal in de strijd met problemen rond digitaal vertrouwen is ook de rol van internationale samenwerking en ratificatie van internationale verdragen om nationale wetgeving vast te stellen, die het mogelijk maakt om activiteiten strafbaar te maken die soms duidelijk onrechtmatig lijken maar geen juridische grond hebben om aangepakt te worden. In Groot-Brittannië zijn pas in mei 2008 nieuwe wetgevende voorstellen aangekondigd om een maas in de wet te sluiten die tekeningen en computer-gegeneerde afbeeldingen van seksueel misbruik van kinderen onbestraft liet.

Door de vier pijlers van Digital Confidence te benoemen wordt het mogelijk het probleem te structureren, prioriteiten te bepalen en het aan te pakken.

De bedrijfstak staat voor de keuze van verschillende niveaus van interventie. Zij moet de eisen van nieuwe businessmodellen en grote investeringen afwegen tegen bredere zorgen over het beleid van het brede publiek en tegen de noodzaak van innovatie en de ontwikkeling van nieuwe diensten en netwerkstrategieën die beantwoorden aan de behoeften en waarden van de "born digital" generatie. De bedrijfstak maakt zich in het algemeen zorgen dat ze zichzelf blootstelt aan onbeheersbare juridische aansprakelijkheden en vertrouwt op de steun van overheidsinstellingen en regelgevers. Afhankelijk van het probleem in kwestie en het land waarin men zich bevindt, kan er geen sprake zijn van een "one size fits all"-benadering om digitaal vertrouwen te stimuleren, maar er kunnen wel belangrijke lessen worden geleerd van best practices. Het gebrek aan een samenhangende aanpak gaat uiteindelijk ten koste van de consument, die transparantie en begeleiding mist rond de risico's en voordelen van de digitale wereld. Bedrijven staan tezelfdertijd voor de uitdaging om duurzame, nieuwe digitale businessmodellen te ontwikkelen.

De moeilijkste aspecten van Digital Confidence liggen niet bij wat er aangepakt moet worden, maar hoe en door wie. De meest geschikte maatregelen moeten worden geformuleerd en verantwoordelijkheden toegewezen – op welk niveau is actie vereist: consument, organisatie, regelgever? En, cruciaal: wie betaalt zulke acties?

Op basis van onze onderzoeken liggen de problemen niet zozeer in de technologische oplossingen, maar meer in de fundamentele, onderliggende beleidskwesties: moet een bedrijf sowieso wel betrokken worden bij bijvoorbeeld het blokkeren van illegale en ongewenste content, met het oog op het risico van juridische aansprakelijkheden? En zo ja, wie maakt uit wat onrechtmatig of "ongewenst" betekent? Waar moet de grens liggen? Als kinderpornografie bijvoorbeeld wordt geblokkeerd, hoe zit het dan met racisme?

Uiteindelijk brengen deze kwesties een hele reeks van belangen met zich mee, zonder simpele antwoorden. De vier benoemde pijlers van Digital Confidence ordenen en structureren de belangrijkste aspecten van het probleem, hetgeen een algemene discussie en aanpak mogelijk maakt.

CONTENTFILTERING

Contentfiltering wordt toegepast om de toegang tot bepaalde (delen van) sites op het internet te beperken. Dataverkeer-/contentfiltering kan worden gebruikt voor veel verschillende doelen, bijvoorbeeld om:

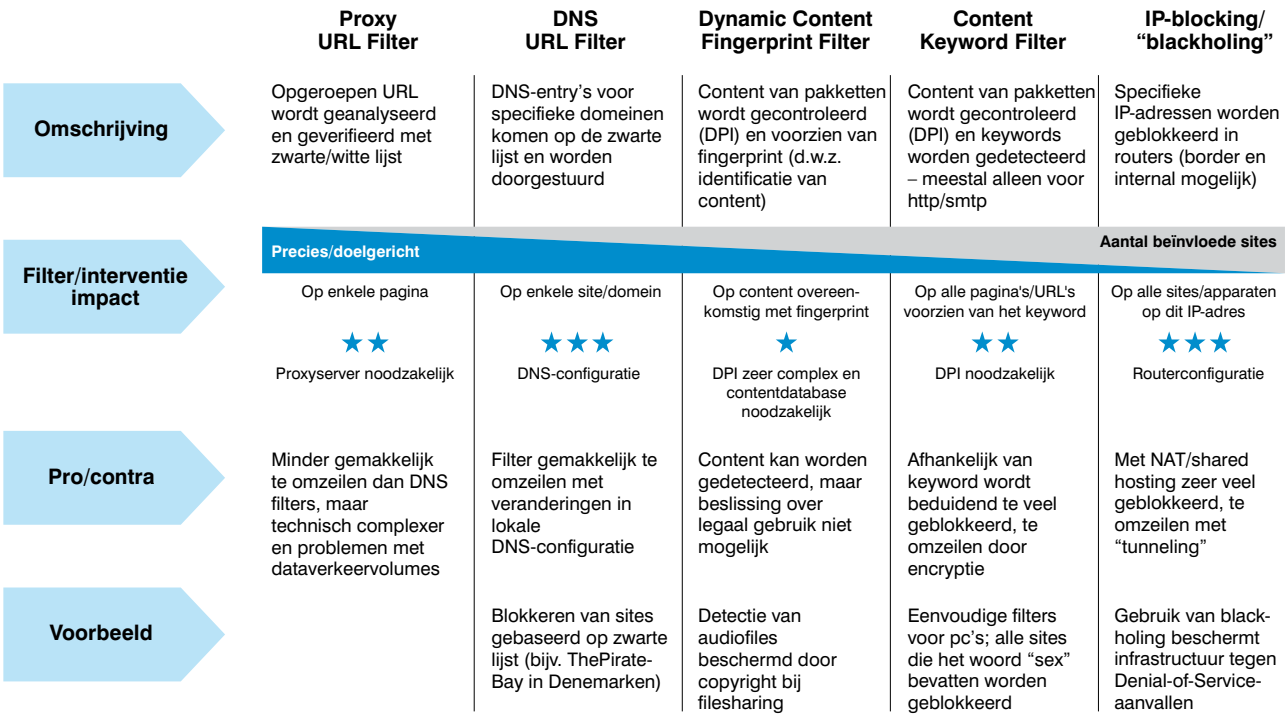
- Spammails te filteren
- Toegang tot illegale content te beperken of blokkeren, zoals kinderpornografie of content die copyright schendt.
- Minderjarigen de toegang te ontzeggen tot ongepaste content

Afhankelijk van het onderliggende motief verschilt de benadering van filtering. In het algemeen kan onderscheid worden gemaakt tussen op de apparatuur van de eindgebruiker gebaseerde filtering (vaak gebruikt als oplossing voor bescherming van minderjarigen, aangezien ouders het gemakkelijk zelf kunnen uitschakelen) en netwerk-gebaseerde filtering (bijvoorbeeld om toegang tot illegale content te beperken of te blokkeren). Een combinatie behoort ook tot de mogelijkheden (bijvoorbeeld voor spamfiltering; mailservers filteren spammail op basis van zwarte lijsten en e-mailprogramma's filteren de rest van de spam op basis van de content).

Voor netwerkfiltering bestaat er een diversiteit aan benaderingen, zoals figuur 35 laat zien. De meest gebruikte implementatie is DNS-gebaseerde URL-filtering.[4)] In dat geval wordt bepaalde

4) DNS is het Domain Name System, waarmee een pc de server voor een bepaald domein kan vinden

Figuur 35: *Verschillende website filters*



Noot: Teneinde omzeiling moeilijker te maken kan naast DNS-gebaseerde filtering niet-extensieve, bijv. poortgebaseerde filtering worden gebruikt

Bron: Booz & Company

★ Moeilijke/dure implementatie

★★★ Eenvoudige/goedkope implementatie

toegang tot het IP-adres behorend bij een specifiek domein geblokkeerd op basis van de domeinnaam ("www.google.com" zou bijvoorbeeld beperkt worden, maar niet "www.google.co.uk", aangezien er verschillende domeinnamen zijn). Dit filter kan zeer eenvoudig door elke netwerkprovider worden geïmplementeerd en is effectief voor alle klanten die de DNS-server van de provider gebruiken.

Nadeel is dat het filter eenvoudig kan worden omzeild door verbinding met een alternatieve DNS-server te maken zonder filters en het kan alleen gebruikt worden voor content op zwarte lijsten. DNS-filtering heeft echter bewezen effectief te zijn bij het voorkomen van onbedoelde of toevallige toegang tot illegale content.

Slimmere filters kijken naar de feitelijke content van het dataverkeer om vast te stellen of het gefilterd moet worden. Een simpel voorbeeld is de detectie van spammails. In dat geval analyseert de mailserver de content van de e-mail.

Een ander voorbeeld zijn simpele "filters van adult-content", die de tekst van een website scannen op sleutelwoorden als "porno" en vervolgens de toegang blokkeren. De meest complexe versies hiervan zijn "Dynamic Content Fingerprinting Filters", die de content van audio- en videodataverkeer kunnen analyseren, bijvoorbeeld om vast te stellen of het om files met copyright gaat. Er bestaan echter controverses over "Deep Packet Inspection", de techniek die vereist is voor deze slimmere filtermethodes. DPI maakt het mogelijk individuele dataverkeer te monitoren, op basis van de toetsaanslagen en mogelijk inclusief e-mailcorrespondentie. Hierdoor zijn zorgen over de privacy ontstaan, aangezien het de mogelijkheid biedt persoonlijke gegevens te verzamelen (bezochte websites, zoekopdrachten) en ook zorgen over onwettig aftappen.

Blackholing is een erg simpel maar uiterst effectief filter – het heeft echter een grote tekortkoming. Blackholing blokkeert de volledige toegang tot een enkel IP-adres (pakketten bedoeld voor dat adres worden niet doorgestuurd) en is lastig te omzeilen, zelfs voor ervaren webgebruikers. Maar aangezien meerdere systemen en websites tot hetzelfde IP-adres kunnen behoren, kunnen door het blokkeren van één IP honderden websites of gebruikers geblokkeerd worden als "collateral damage" (overblokkeren genaamd). Deze maatregel wordt daarom alleen gebruikt als de integriteit van grote netwerken gevaar loopt of als gebruikers een groot risico lopen als blackholing niet wordt toegepast.

In het algemeen kunnen filtermaatregelen alleen effectief zijn als lijsten met illegale content worden beheerd, onderhouden, regelmatig geactualiseerd en goed toegepast. Toch staan er beleidsimplicaties voor een groter publiek op het spel, als lijsten verder reiken dan hun oorspronkelijke doel en in gevallen waarbij illegale content niet tijdig wordt verwijderd.

IV. HUIDIGE AANPAK VAN DIGITAL CONFIDENCE: AANZIENLIJKE RUIMTE VOOR VERBETERING

Teneinde een coherent raamwerk te ontwikkelen voor het veiligstellen van Digital Confidence, is het essentieel de verschillende benaderingswijzen door de diverse belanghebbenden onder de loep te nemen.

Een aantal casestudies wordt besproken om best (en worst) practices te begrijpen en er lessen uit te trekken. De beschouwing van de casestudies wordt vervolgens aangevuld met een korte bespreking van de agenda van de regelgevers waar het gaat om Digital Confidence.

1. CASE STUDIES: HOE DIGITAL CONFIDENCE TE LATEN SLAGEN – OF NIET

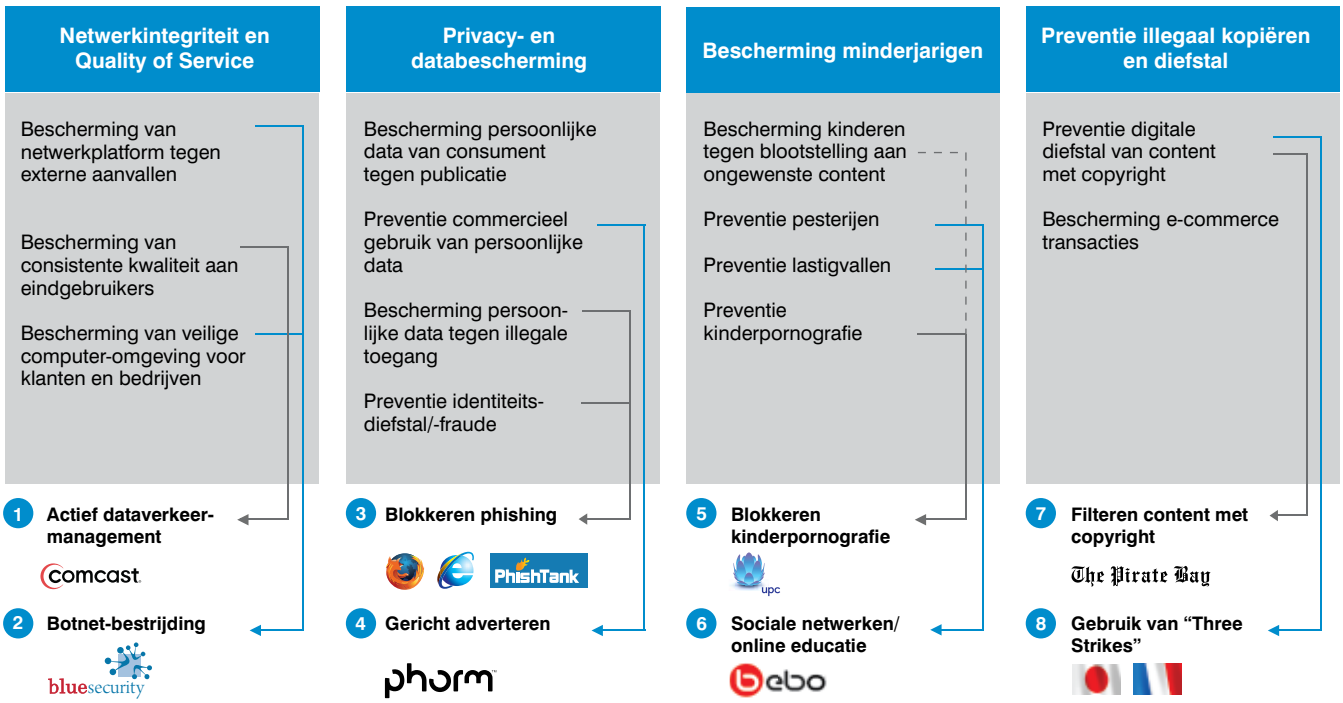
De cases worden gerangschikt aan de hand van de vier Digital Confidence-pijlers – Netwerkintegriteit en Quality of Service, Privacy- en databescherming, Bescherming van minderjarigen en Preventie van illegaal kopiëren en diefstal. Per pijler zijn twee cases geselecteerd om de doelstellingen van elke pijler zo duidelijk mogelijk te maken en goed onderbouwde conclusies mogelijk te maken (figuur 36):

- "Learning potential"
- Tijdigheid
- Geografische diversiteit

Zoals nader besproken in hoofdstuk III, is een van de grootste problemen de algemene positie die een organisatie inneemt op een specifiek gebied van Digital Confidence: hoe beschermend of zelfs dwingend wil of moet ik zijn? Hoe opdringerig kunnen de gebruikte maatregelen zijn?

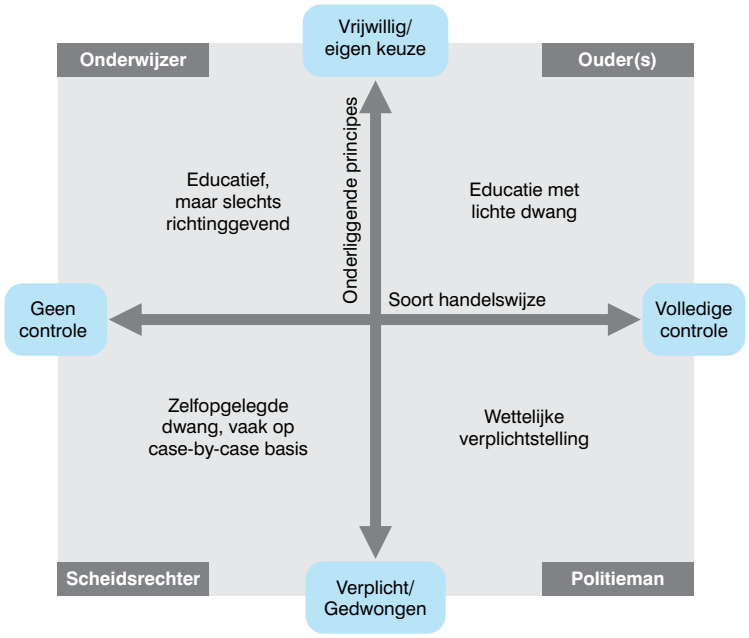
Om de cases te onderzoeken is een generiek "Digital Confidence Positioneringsmodel" ontwikkeld (figuur 37). Binnen dit model toont de horizontale as hoe maatregelen worden genomen (bijvoorbeeld passief op een "hands-off"-manier, of actief volgens een "volledige controle"-benadering), terwijl de verticale as de onderliggende principes differentieert. Vanuit de hieruit voortvloeiende vier kwadranten kan duidelijk een verband gelegd worden

Figuur 36: *Voorbeelden van huidige methodes*



Noot: Kleur van de pijlen uitsluitend ter onderscheid
Doorgetrokken lijn = belangrijk aspect; stippellijn = minder belangrijk aspect

Figuur 37: *Digital Confidence positioneringsmodel*



met generieke maatschappelijke rollen. Bijvoorbeeld:

- De onderwijzer informeert gebruikers zoveel mogelijk over mogelijkheden en bedreigingen, maar zal doorgaans niet actief corrigerend optreden (voorbeeld: "Web Wise Kids" met informatief materiaal voor kinderen op het internet).

- De ouder informeert evenals de onderwijzer gebruikers over bedreigingen en maatregelen, maar treedt proactief op als gebruikers beschermd moeten worden (bijv. YouTube dat auteursrechtelijk beschermde content filtert).

- De scheidsrechter vertrouwt van geval tot geval eerder op zelfopgelegde handhaving van regels en richtlijnen dan op voorlichting, maar die regels zijn gebaseerd op wederzijdse instemming (bijv.: UPC NL dat proactief toegang beperkt tot internetdomeinen met seksueel kindermisbruik).

- De politieagent is van nature geneigd wetgeving strikt uit te voeren, alle noodzakelijke maatregelen te nemen en doet dat op basis van strikte regels, zoals alle onwettige activiteiten blokkeren (bijv. implementatie van een "three strikes you're out" regel bij schending van auteursrechten).

CASE 1: ACTIEF DATAVERKEER-MANAGEMENT

Probleem: ***Netwerkproviders worden geconfronteerd met steeds toenemend gebruik van bandbreedte. Ze moeten dataverkeer managen om netwerkcongestie te voorkomen en Quality of Service zeker te stellen.***

Risico: ***Quality of Service (QoS) kan in gevaar komen door pieken in de vraag naar bandbreedte – maar het upgraden van de netwerkbandbreedte alleen zou onoverkomelijk duur zijn, terwijl het geen oplossing voor de lange termijn biedt.***

Zware gebruikers consumeren grote hoeveelheden bandbreedte ten koste van reguliere gebruikers. Toepassingen als filesharing en streaming video vergen veel meer bandbreedte dan het gebruikelijke browsen of e-mail. Deze uiteenlopende intensiteit vertaalt zich in sterke pieken in het gebruik van de totale capaciteit van welk netwerk dan ook. Netwerkproviders pakken dit aan door te investeren in Next Generation toegangsnetwerken om de capaciteit voor de eindgebruikers voortdurend uit te breiden. Maar om alle gebruikers optimale Quality of Service (QoS) te bieden is meer nodig. Steeds meer zware gebruikers gebruiken steeds meer bandbreedte, waardoor alleen het uitbreiden van de capaciteit niet meer kan zijn dan een kortetermijnoplossing tegen de verstopping van bandbreedte. Daarom moet dataverkeer ook gemanaged worden om een "billijke" verdeling van de bandbreedteconsumptie en QoS voor alle gebruikers (figuur 38) te verzekeren. Bij hantering van eenvormige prijsstellingen - flat-fee tarieven - worden gebruikers met een grote consumptie (steile deel van de curve) "gesubsidieerd" door gebruikers met een geringe consumptie. Ter verduidelijking: als dataverkeer van 10 procent van de zware downloaders zou worden geshaped of als ze gemigreerd naar "zwaardere" abonnementen tegen hogere tarieven zouden worden, zou de "eerlijkheid" in de verdeling van beschikbare bandbreedte voor alle gebruikers toenemen met bijna 50 procent.

Gedifferentieerde tarifering en maatregelen op het gebied van dataverkeermanagement zijn de twee belangrijkste remedies. Gedifferentieerde tarifering kan grootgebruikers aansporen hun netwerk-gebruik te beperken door downloaden tijdens piekuren extra te belasten, zeker voor toepassingen die veel bandbreedte opeisen, zoals filesharing. Deze extra kosten hebben twee effecten: ten eerste verschuiven ze de vraag weg van de piekuren en ten tweede zorgen ze voor extra opbrengsten die kunnen bijdragen aan het bekostigen van uitbreiding van de infrastructuur.

De Canadese kabeloperator Rogers introduceerde gedifferentieerde tarifering, AT&T onderzoekt een speciaal prijsmodel voor BitTorrent-dataverkeer om de invloed van P2P-dataverkeer op het netwerk terug te dringen (het bedrijf verwacht dat het totale bandbreedtegebruik op zijn netwerk met een factor vier zal toenemen gedurende de komende drie jaar) en Time Warner test een prijssysteem dat de kosten voor de gebruikers berekent op grond van de door hen geconsumeerde bandbreedte.

Maatregelen voor dataverkeermanagement sturen aan op een brede reeks netwerkgedreven maatregelen, bedoeld om het dataverkeer te faciliteren en Quality of Service veilig te stellen – aangevuld door het dimensioneren van het netwerk in brede zin, met name om piekbelastingen aan te pakken. Maatregelen strekken zich uit van het handhaven van "eerlijk gebruik"-limieten tot verschillende vormen van "shaping", met verschillende benaderingen van dataverkeerselectie om de beste QoS zeker te stellen (zie ook hoofdstuk III).

De manier waarop spelers dataverkeermanagement benaderen, kunnen worden besproken met verwijzing naar een aangepaste versie van het generieke Digital Confidence Positioneringmodel (figuur 38). De verticale as differentieert de algemene positie die een netwerkoperator of ISP kan innemen ten aanzien van dataverkeermanagement. Hierbij is de bovenste pool een positie die stimulansen biedt maar geen invloed uitoefent op de feitelijke gebruikersactiviteit, terwijl de onderste pool een gedwongen positie weergeeft die actief reageert op dataverkeer en het beheert, op basis van de totale gebruikersactiviteit op een bepaald moment. De horizontale as differentieert de mate waarin feitelijke dataverkeerdata de ondernomen acties bepalen, d.w.z. hoe specifiek de genomen technische maatregelen zijn. Servicespecifieke shaping maakt minder nauwkeurig onderscheid tussen verschillende soorten dataverkeer dan bijvoorbeeld protocolspecifieke shaping.

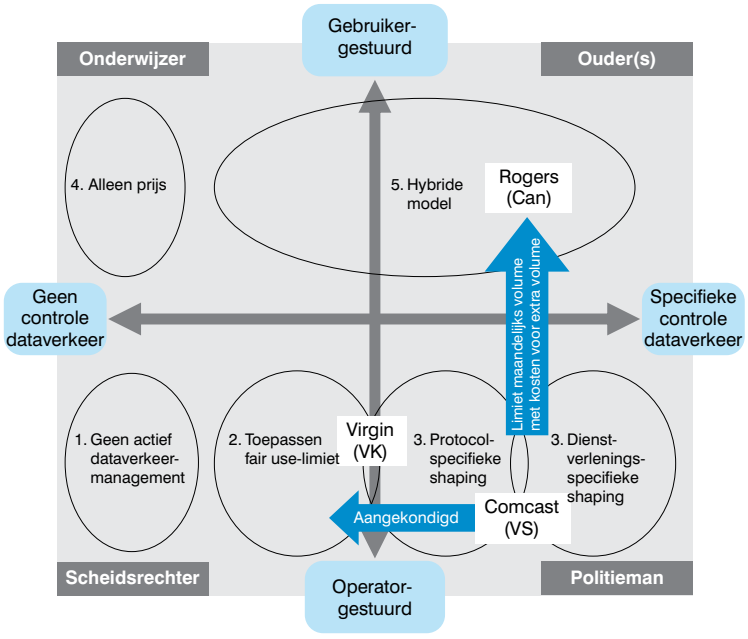
Bepaalde posities in de matrix zijn natuurlijker dan andere: het is bijvoorbeeld onwaarschijnlijk dat een "alleen prijsstelling"-benadering, zoals in het onderwijzer-kwadrant, bestaat, gezien de huidige onbalans tussen beschikbare bandbreedte en vraag – netwerkoperators kunnen geen goed functionerend netwerk garanderen zonder enige technische maatregelen of dataverkeermanagement.

Enkele recente handelswijzen in de matrix vielen op. Comcast, een van de grootste kabeloperators in de Verenigde Staten, zag een aanzienlijke toename van dataverkeer door toegenomen gebruik van P2P-systemen. Onder deze druk scherpte Comcast zijn dataverkeermanagement aan en het publiek verzette zich sterk. Rogers, in Canada, introduceerde tegemoetkomingen voor gebruikers, waarbij zij extra kosten in rekening brachten voor dataverkeer boven

*"Niet-beheerde netwerken leiden tot slechtere dienstverlening en kwaliteit voor alle gebruikers. Bovendien betalen klanten meer voor minder omdat providers hun netwerken moeten blijven uitbreiden om de enorme groei in bandbreedteconsumptie vóór te blijven." **

* Kurt Dobbins, Arbor Networks

Figuur 38: *Digital Confidence positie t.a.v. actief dataverkeermanagement*



1. Enkele netwerkoperators managen niet actief hun dataverkeer
   – Pro: Bij voldoende reservecapaciteit is er geen echte noodzaak voor actief dataverkeermanagement
   – Contra: Geen gegarandeerde user experience – mogelijke netwerkcongestie
2. Netwerkoperators gebruiken "Fair Use"-regels, gebaseerd op een bepaalde netwerk capaciteit om piek uren te kunnen opvangen
   – Gebruikers die Fair Use-limieten overschrijden kunnen worden gemigreerd naar andere (hogere bandbreedte) abonnementen
3. Actief dataverkeermanagement wordt ingezet om QoS voor alle gebruikers te garanderen
   – Vanuit een netneutraal standpunt gezien, is een niet-dienst-specifieke benadering te prefereren boven een dienst-specifieke benadering
4. Een ander zakelijk alternatief voor bandbreedte-management is prijsdifferentiatie, gebaseerd op gebruik
   – Pro: Door de markt gesteunde aansporing om congestie te managen door excessief gebruik te ontmoedigen
   – Contra: Ondermijnt gebruiksgemak en mogelijk competitief nadeel
5. Hybride modellen gebruiken prijsdifferentiatie als het gebruik bepaalde limieten/capaciteiten overschrijdt
   – Gemiddelde gebruiker profiteert nog steeds van "flat fee"-gemak – alleen zware gebruikers betalen extra

bepaalde limieten (2 tot 100 GB per maand). Dit is een voorbeeld van een hybride benadering, waarbij dataverkeermanagement gecombineerd wordt met gedifferentieerde tarifering. Daarnaast is Virgin Media in Groot-Brittannië een voorbeeld van een kabeloperator die erg open is over haar activeiteiten ten aanzien van dataverkeermanagement.

*"Waar het dus echt om gaat bij de breedbandnetwerken van vandaag, is niet of ze gemanaged moeten worden, maar hoe." **

Comcast implementeerde maatregelen voor netwerkmanagement voor P2P-dataverkeer van BitTorrent, die te beperkend bleken: downloaden van BitTorrent was mogelijk, maar gebruikers meldden vertraging bij uploads en dat de implementatie ook andere, meer tijdgevoelige toepassingen beïnvloedde, zoals Lotus Notes. Individuele gebruikersklachten leidden uiteindelijk tot brede publieke aandacht, waaronder een onderzoek door de FCC. Comcast werd ook beschuldigd van misleidende servicebeloften en computerfraude.

Sommige spelers, zoals Virgin Media en Rogers, zijn zeer transparant over hun benadering van dataverkeermanagement – de acceptatie lijkt groot.

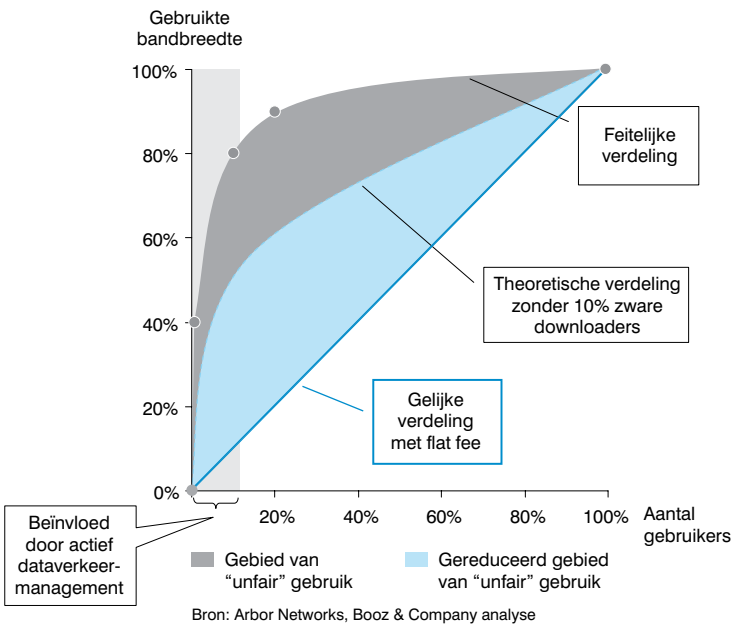
Als antwoord pakte Comcast het probleem daadkrachtig aan, werkte samen met BitTorrent en vond een voor beide partijen aanvaardbare oplossing: Comcast zal een protocol-onafhankelijke techniek gebruiken die uiteindelijk alleen de P2P-dataverkeer van zware gebruikers zal vertragen. Deze overeenkomst lijkt goedgekeurd te worden door voorstanders van netneutraliteit. Google noemde Comcast's protocol-onafhankelijke benadering van netwerkmanagement "een stap in de goede richting". Het stelde de FCC echter niet tevreden en die besloot de eerdere praktijken van Comcast te veroordelen.

De FCC is voorstander van "redelijk" netwerkmanagement, maar beweerde dat Comcast willekeurig internettoegang blokkeerde zonder oog te hebben voor de mate van dataverkeer en er niet in slaagde zijn standpunt duidelijk te maken aan de consumenten. In juli 2008 adviseerde het hoofd van de FCC om tot actie over te gaan. Hij eiste dat Comcast zou stoppen met zijn "blokkeerpraktijken" (hoewel "vertraging" waarschijnlijk een betere omschrijving is). Comcast zou verder de consument informatie moeten geven over de reikwijdte van - en de manier waarop de methodes waren gebruikt en de consumenten details geven over de toekomstplannen van de onderneming om zijn netwerk te managen. Deze actie volgt een FCC-besluit uit 2005 waarin een aantal principes werden geformuleerd om te garanderen dat breedbandnetwerken "op grote schaal openstaan, betaalbaar zijn en toegankelijk voor alle consumenten". De principes zijn echter wel "onderhevig aan redelijk netwerkmanagement". Het FCC besluit ten aanzien van Comcast lijkt meer een principekwestie – ook al omdat Comcast waarschijnlijk niet beboet kan worden – en lijkt een precedent te willen scheppen om nader te kunnen bepalen wat "redelijk netwerkmanagement" in de praktijk betekent.

Rogers introduceerde in maart 2008 gebruikstoeslagen. Gebruikers moeten afhankelijk van hun tariefgroep $1,25 tot $5 per maand extra betalen, geldend voor alle groepen. Steeds meer netwerkproviders overwegen de introductie van gebruikgebaseerde prijsmodellen om de toenemende vraag naar bandbreedte te managen. Het probleem met deze gefaseerde benadering is dat het de basisbelofte van een "flat fee" kan ondermijnen, wat toch de belangrijkste aandrijver was van de ontwikkeling van de breedbandmassamarkt, namelijk vrij breedbandgebruik zonder zorgen over toenemende kosten door niet te controleren gebruik. Rogers pakt dit probleem aan met de $25 "cap". Rogers is zelf zeer open en pretentieloos over zijn beleid en vermeldt op de website: "De meerderheid van onze klanten bevindt zich in een categorie die voldoet aan hun behoeften en hoeft niet te verwachten meer te gebruiken dan ze maandelijks is toegewezen. Als u die toch overschrijdt, kunt u maandelijks betalen voor extra gebruik, of uw servicepakket zo aanpassen dat het aan uw online-behoeften voldoet. Gebruik op deze manier meten geeft eerlijker weer hoe onze klanten de dienst gebruiken en stelt ons in staat concurrerende prijzen te handhaven voor al onze klanten."

* *Vint Cerf, Chief Internet Evangelist, Google*

Figuur 39: *Bandbreedteconsumptie door gebruikersgroepen*



Bron: Arbor Networks, Booz & Company analyse

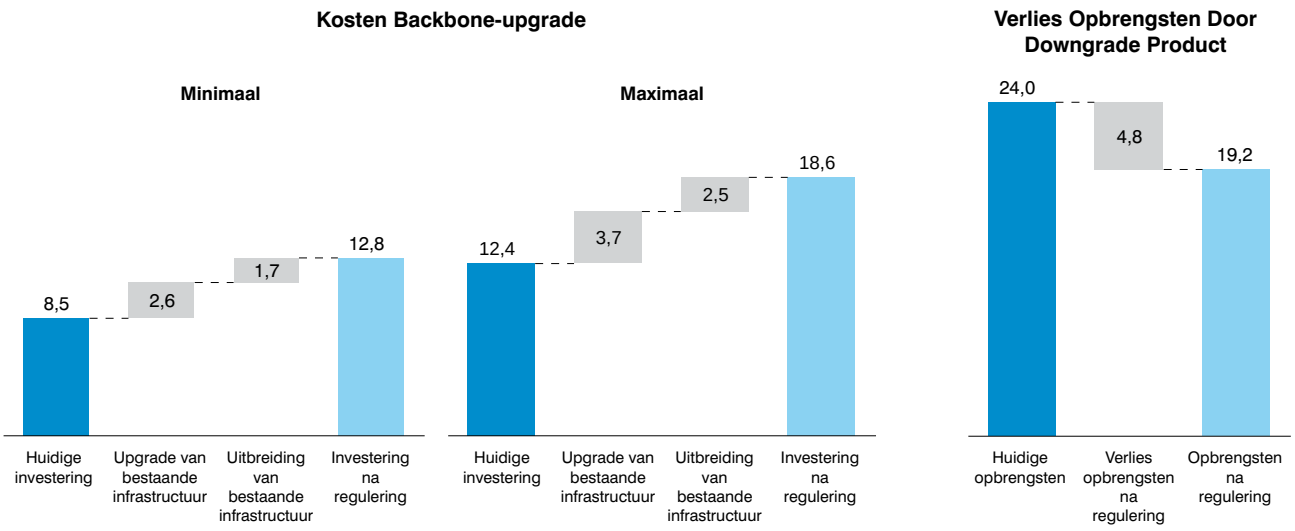
In Groot-Brittannië is Virgin Media eveneens erg open over de behoefte aan dataverkeermanagement en de gekozen implementatie. Momenteel gebruikt Virgin dataverkeer-shaping om de 3 procent zwaarste gebruikers te managen – de toegepaste regels zijn openbaar beschikbaar op de website. Virgin Media plaatst zijn maatregelen in de context van een "eerlijk gebruik"-beleid en stelt zo de Quality of Service veilig voor de overgrote meerderheid van gebruikers. Virgin overweegt ook de introductie van prijsgebaseerde modellen in de toekomst.

IMPLICATIES VAN BEPAALDE REGULERENDE ALTERNATIEVEN VOOR MINIMUM QOS-VEREISTEN

Figuur 40: *Varianten van mogelijke Quality of Service-regulering*

0. Shaping niet toegestaan	1. Geringe QoS-vereisten	2. Middelmatige QoS-vereisten	3. Hoge QoS-vereisten
• Netneutraliteit kan worden geïnterpreteerd als belemmering voor dataverkeer-shaping in het netwerk • Dit kan in potentie worden gecombineerd met andere opties, maar is erg moeilijk te realiseren	• Kan worden geïmplementeerd door bestaande netwerk-management-oplossingen – Shaping gebaseerd op service/protocol – Min of meer agressieve shaping	• Bijv. minimale bandbreedte of gematigde latency-vereisten • Kan worden geïmplementeerd binnen bestaande infrastructuur en geringe upgrades – Backbone-upgrades voor meer bandbreedte en minder shaping – Toegangs-upgrades (nieuwe CPE)	• Hoog QoS-vereiste (minimale bandbreedte, in combinatie met geringe latency en jitter) • Bestaand netwerk voldoet niet aan vereisten; nieuwe technologieën moeten worden geïmplementeerd
• Service providers die momenteel shaping toepassen, hebben twee mogelijke opties – Backbone upgraden – Producten downgraden	• Geen backbone- of toegangs-upgrades noodzakelijk	• Backbone- of toegangs-upgrades noodzakelijk voor delen van het netwerk • Verschilt voor DSL en kabel: afwijkende technische restricties (kabel met gedeelde toegang kan bijv. eenvoudig meer bandbreedte leveren, maar vatbaarder voor congestie)	• Backbone- en toegangsupgrades noodzakelijk (in feite netwerk opnieuw opbouwen)
Product downgraden of backbonenetwerk upgraden	**Geen upgrades**	**Netwerkupgrade**	**Netwerk "opnieuw opbouwen"**

Figuur 41: *Financiele gevolgen van "niet-shaping"-regulering in Europa (in miljarden euro's)*



Noot: Europa: EU-27 + Noorwegen + Zwitserland
Noot: Dit is een hypothetisch scenario, er vanuit gaande dat shaping niet is toegestaan in Europa en momenteel 20% van alle dataverkeer is geshaped en op basis van 67% dataverkeergroei p.j. (niet uitgaande van enige verdeling van shaping tussen spelers onderling)
Bron: US BEA, Merrill Lynch, Ofcom, Bedrijfsrapportages, Booz & Company analyse

Dataverkeermanagement trekt steeds meer kritische aandacht van regelgevers. Het FCC-besluit inzake Comcast onderstreept het feit dat consumentenbescherming hoog op de agenda staat bij het definiëren van "redelijk" dataverkeermanagement. Maar het is een complex onderwerp gezien vanuit regulerend oogpunt. De figuren 40 en 41 laten zien wat de economische invloed van regelgevende beslissingen kan zijn in die context. Het opleggen van zeer strikte Quality of Service regels die van invloed zijn op de mate waarin dataverkeermanagement wordt toegepast, kan aanzienlijke extra kosten met zich meebrengen voor de bedrijfstak in Europa. Kosten die niet door de netwerkproviders kunnen worden opgebracht en dus noodgedwongen leiden tot hogere prijzen voor de eindgebruiker. Uiteindelijk kan excessief gebruik door een tamelijk klein consumentensegment leiden tot een algemene kostenstijging voor de eindgebruiker. Daarom dient regulerend optreden met betrekking tot dataverkeermanagement zorgvuldig te worden afgewogen.

BELANGRIJKE LESSEN
Uit het bovenstaande komen vijf belangrijke lessen naar voren:

- Het beheren van netwerkcongestie en capaciteitsbeperkingen is een essentieel onderdeel van de bedrijfsvoering van elke netwerkoperator – gedifferentieerde tarifering en maatregelen voor dataverkeermanagement zijn de twee belangrijkste remedies.

- Naar verwachting zal de gebruiksgroei gelijke tred houden met de toename van bandbreedtes in Next Generation toegangsnetwerken. Dit vergroot het probleem, aangezien zwaar gebruik van veel bandbreedte vereisende toepassingen zal toenemen. Extra kosten rekenen voor zwaar gebruik draagt wellicht bij aan evenwichtiger internetverkeer en een eerlijke verdeling van bandbreedte voor alle gebruikers.

- Maatregelen voor dataverkeermanagement zijn altijd in zekere mate noodzakelijk en zijn geschikt om Quality of Service voor alle soorten dataverkeer te garanderen; openbare transparantie over deze methodes is noodzakelijk om te voldoen aan verwachtingen op het gebied van serviceverlening.

- De implementatie van dataverkeermanagement maatregelen moet het debat over netneutraliteit in acht nemen – protocol-specifieke implementaties (zoals BitTorrent) kunnen rekenen op forse kritiek van het publiek. Protocol-onafhankelijke "fair use"-handhaving lijkt dan ook het eerlijkst als het buitensporig gebruiksgedrag beheert en direct is gericht op – en beperkt tot – het beheren van de mate van dataverkeer ten tijde van feitelijke congestie. Deze benadering biedt wellicht de beste QoS-ervaring in brede zin en een interventieniveau dat strookt met netneutraliteit.

- Problemen in verband met dataverkeermanagement kunnen wellicht effectief bestreden worden door wederzijds aanvaardbare en transparante overeenstemming te bereiken tussen netwerkoperators en bijvoorbeeld leverancier van toepassingen. De mate van breedbandconcurrentie in een bepaalde markt zou de behoefte aan regulerende interventie moeten bepalen.

CASE 2: BOTNET-BESTRIJDING
***Probleem:* Steeds meer consumentencomputers raken besmet door bots, kwaadaardige software die op afstand bestuurd kan worden door criminelen ("botherders"). Ter bescherming van consumenten en netwerken willen ISP's deze bots van het internet verwijderen.**
***Risico:* Botnets zijn de grootste veroorzakers van de meeste digitale aanvallen, zoals phishing, spam, klikfraude, etc.**

Vermoedelijk zijn botnets de ernstigste vorm van criminele inbreuk op netwerkintegriteit:

P4P als manier om P2P-dataverkeer in te perken en de kwaliteitsbeleving voor gebruikers te verbeteren

P4P is de "Proactive Network Provider Participation for P2P", een initiatief van de DCIA (Distributed Computing Industry Association). De kern van de werkgroepleden bestaat uit vooraanstaande spelers: AT&T, BitTorrent, Cisco, Joost, Pando, Telefonica, Verizon en Vuze.

P4P heeft twee doelen: (i) backbone-verkeer terugdringen, en ii) verhinderen van netwerkkosten. Het technische idee is een P2P-systeem te bouwen (gebaseerd op BitTorrent) dat extra informatie over de netwerktopologie gebruikt om de peers te selecteren om data mee uit te wisselen. Om dit te bereiken gebruikt de ISP extra tracker-servers om beschikbare peers te rangschikken op basis van optimale routes.

Verder is het idee van caches op ISP-niveau geïntroduceerd – waarmee de hoeveelheid data wordt gereduceerd die omgeleid wordt en toegang mogelijk maakt (klanten uploaden slechts eenmaal data naar de cache, die alle verzoeken in het netwerk kan doorvoeren). Eerste testen met Pando (BitTorrent-gebaseerd) tonen een snelheidswinst van 200 tot 800 procent en een afname van 40 tot 70 procent in het dataverkeer tussen ISP's.

een botnet is een verzameling computers bij mensen thuis, op bedrijven, universiteiten en dergelijke die op afstand ongemerkt worden bestuurd door een onbevoegde kwaadwillende derde. Botnets kunnen enkele honderdduizenden computers omvatten.

Botnets kunnen worden gebruikt voor onder meer spammen en Denial of Service- (DoS)[5] aanvallen tot phishing en klikfraude. Enkele recente voorbeelden tonen hoe groot de gevolgen van deze botnetaanvallen kunnen zijn. In april 2007 werd – nadat in Tallinn, de hoofdstad van Estland, een Russisch standbeeld was verwijderd – een "handmatige" DoS-aanval georganiseerd: bloggers vroegen hun lezers om specifieke Estlandse services te "pingen" om zodoende een DoS te creëren. Een "ping" is een software-utility die een pakketje data naar een bepaald IP-adres stuurt om te bepalen of dat adres beschikbaar is. Het is in de eerste plaats bedoeld om internetverbindingen te repareren, maar kan zo ook misbruikt worden. De aanval mislukte, er werd een botnet "gehuurd" en vervolgens werd een "echte" DoS-aanval gelanceerd. Doelwitten waren onder meer websites van de Estlandse regering en het parlement, ministeries, politieke partijen, twee van de zes grootste ondernemingen van het land, twee van de grootste banken en firma's gespecialiseerd in communicatie. De aanval haalde letterlijk de digitale kant van het leven "uit de lucht" in een land waar 90 procent van de banktransacties online plaatsvindt.

*Kraken is een van de grootste bekende botnets **

In april 2008 beleefde Radio Free Europe, een non-profitorganisatie gesticht door de Verenigde Staten, een enorme DoS-aanval. Meerdere Oost-Europese websites van Radio Free Europe werden aangevallen, dat wil zeggen overspoeld door namaakverzoeken (zodat alle middelen werden gebruikt door de DoS-aanval). Beide aanvallen waren feitelijk politiek van aard en kwamen tot stand door (vaak "gehuurde") botnets.

Aangezien de meeste doeleinden van botnets onrechtmatig zijn, speelt juridische vervolging een grote rol bij de bestrijding ervan. In de Verenigde Staten voerde de FBI in de zomer van 2007 de operatie "Bot Roast" uit waarbij circa één miljoen misbruikte computers werden geïdentificeerd en talloze cybercriminelen is staat van beschuldiging werden gesteld. Naast vervolging zijn er helaas slechts weinig mitigerende strategieën tegen botnets – besmetting voorkomen is zeer effectief, maar ook moeilijk.

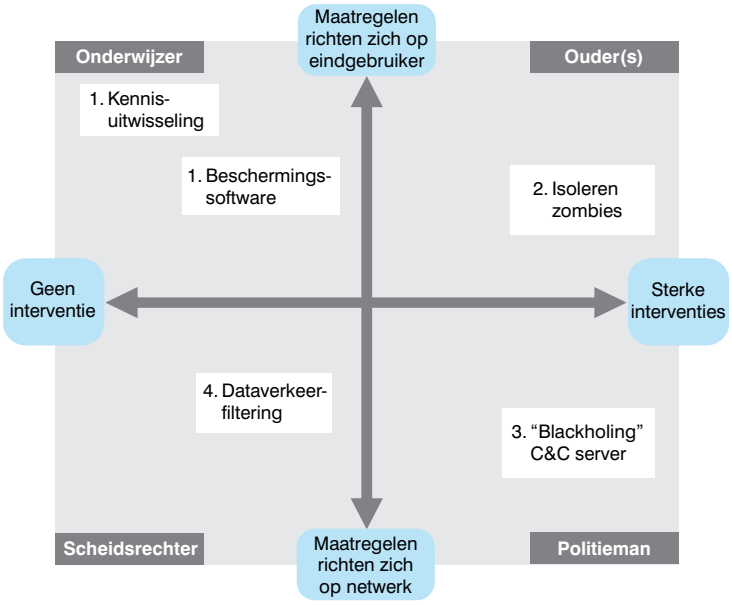
Het bestrijden van botnets op een "niet-vervolgende" manier kan vorm krijgen aan de hand van een aangepaste versie van het generieke Digital Confidence Positioneringmodel (figuur 42). De verticale as differentieert waar bestrijding plaatsvindt: bij de eindgebruiker of bij het netwerk. De horizontale as differentieert de kracht van de interventie. De linker pool staat voor helemaal geen interventie, de rechter voor sterke interventie.

Voorlichting is een duidelijk voorbeeld van een maatregel zonder tussenkomst gericht op

5) Noot: In dit document wordt de term DoS gebruikt, hoewel technisch gezien de aanvallen van botnets DDoS-aanvallen zijn (Distributed Denial of Service-aanvallen).

** 500.000 besmette pc's, 50 Fortune 500-bedrijven getroffen*

Figuur 42: *Digital Confidence positie t.a.v. bestrijden botnets*



1) Wordt normaal alleen gebruikt voor control-servers en DoS-machines, maar niet voor geïnfecteerde pc's

1. De meeste ISPs geven gebruikers voorlichting en geschikte beschermingssoftware
   - Pro: Kan bot-infectie voorkomen
   - Contra: Softwarebescherming niet 100% zeker en enige technische voorkennis nodig
2. Isoleren van geïnfecteerde pc's van het internet in een 'walled garden' vindt zeer sporadisch plaats
   - Pro: "Garden" minimaliseert verspreiding van botnets
   - Contra: Aansprakelijkheidsproblemen bij valse verdenking en zeer service-intensief
3. "Blackholing" betekent in principe machines afsluiten van het internet [1]
   - Pro: Zeer effectief, met name voor oudere botnets (of DoS-aanvallen)
   - Contra: Extreme maatregel, aangezien alle dataverkeer wordt geblokkeerd
4. Filteren botnet dataverkeer – zeer effectief, maar moeilijk te implementeren
   - Pro: Minimaliseert bedreiging met weinig verstoring van andere activiteiten
   - Contra: Botnet-dataverkeer moeilijk te filteren door sterke gelijkenis met normale internetdataverkeer

de gebruiker: zorgen dat eindgebruikers botnet-risico's begrijpen en weten wat ze ertegen kunnen doen. ENISA (European Network and Information Security Agency) publiceerde bijvoorbeeld voorlichtingsmaterialen over botnets, de gevaren en hoe consumenten zich ertegen kunnen besschermen.

Een andere maatregel in het onderwijzerkwadrant is software die computers tegen botnet-infectie beschermt. Bijna alle huidige commerciële antivirus- en firewallproducten bieden bescherming tegen besmetting. Leveranciers hiervan zijn zelf ook kwetsbaar: in mei 2006 werd Blue Security, een klein bedrijf gespecialiseerd in beveiligingssoftware, uit de markt gedrukt door een enorme DoS-aanval.

Blue Security had een volgens zeggen zeer effectief antispam-product op de markt gebracht – ironisch genoeg ook gebaseerd op het principe van botnet.[6)] Blue Security werd daarop door spammers gechanteerd om te stoppen. Toen Blue Security dit weigerde, werden de servers platgelegd door een DoS-aanval. De beheerders verlegden de DNS-entry naar TypePad, een van de grootste bloghosts, ook gebruikt door Blue Security. Massale DoS-aanvallen die daarop volgden legden zelfs TypePad en Tucows, de DNS-provider van Blue Security, tijdelijk plat; twee grote en belangrijke websites. Slechts dankzij gecoördineerd ingrijpen van meerdere netwerkoperators en serviceproviders konden de aanvallen, met pieken van 3 GB/s, worden bestreden en derden worden beschermd. Blue Security was echter meerdere dagen offline. Twee weken na de eerste aanval stopte Blue Security met de antispam-afdeling.

*Blue Security CEO Eran Reshef over spambestrijding: "Hier moeten de autoriteiten over beslissen. Om spammers te bestrijden moet je echt $100 miljoen uitgeven." **

Een meer op de eindgebruiker gerichte maar interventionistische aanpak is het afsplitsen van de zombies, de individuele computers in een botnet. Dit is een krachtige maar moeilijke bestrijdingsmaatregel, geopperd door de MAAWG (Message Anti-Abuse Working Group). Besmette computers worden afgezonderd van het internet en in een "ommuurde tuin" geplaatst, met veiligheidsupdates en ontsmettingsmogelijkheden. Tot dusver is dit slechts zeer sporadisch toegepast, bijvoorbeeld bij grote privé-netwerken zoals universiteiten, vanwege mogelijke aansprakelijkheidsproblemen.

De meest effectieve maatregel was altijd de command en control- (C&C) server te blackholen/ontkoppelen. Zo ontwrichtte de Noorse ISP Telenor al in 2004 een botnet van 10.000 zombies door de C&C-server uit te schakelen. Maar botherders kwamen met een antwoord en gebruiken steeds vaker nieuwe types botnets, zonder centrale C&C-server.

Ten slotte zijn er filtertechnieken van dataverkeer om botnets te bestrijden: ook netwerkgedreven, maar veel minder interventionistisch. Ook hier is het doel van het filteren om ongewenste botnet-dataverkeer te herkennen en dan hun IP-pakketten te blokkeren, zodat ze hun doel niet kunnen bereiken. Het probleem hier is dat botnet-dataverkeer erg moeilijk te filteren is, omdat het zoveel lijkt op normaal internetverkeer. Veel ISP's en netwerkoperators gebruiken tegenwoordig een eenvoudigere vorm: ze blokkeren alle dataverkeer die kenmerkend is voor botnets – met het gevaar dat ze rechtmatige gebruikers ook overblokkeren.

Verder bundelen ISP's ook steeds meer hun krachten met de wetgever door het netwerk te monitoren en onregelmatigheden te melden. Op deze manier werd in Nederland in 2005 een grote botnet uit de lucht gehaald toen internetprovider XS4ALL de autoriteiten op de hoogte stelde van "ongebruikelijke activiteit op zijn netwerk". Het bestond uit 1,5 miljoen zombies en drie verdachten werden in staat van beschuldiging gesteld.

BELANGRIJKE LESSEN

Uit het bovenstaande kunnen zeven belangrijke lessen worden getrokken:

- Door hun openheid en neutraliteit zijn IP-netwerken zeer krachtig, maar tevens gemakkelijk bruikbaar voor "kwaadwillige bedoelingen", zoals botnets.

- Door hun veelzijdigheid in mogelijke aanvallen vormen botnets een grote bedreiging voor netwerkintegriteit en dus voor netwerkoperators, serviceproviders, bedrijven en consumenten – vaak hebben botnets ook een politieke achtergrond, zoals de voorbeelden van Estland en Radio Free Europe duidelijk maken.

- Een van de ernstigste aanvallen is de Denial of Service-(DoS)aanval om ongewenste sites uit de lucht te halen of bedrijven te chanteren – botnets zijn verantwoordelijk voor alle grote DoS-aanvallen in de afgelopen jaren.

- Juridische vervolging speelt een belangrijke rol in de bestrijding van botnetactiviteiten – maar om succesvol te zijn moeten andere belanghebbenden, met name netwerkoperators en ISP's, daar wel aan meewerken.

6) Als Blue Frog een spammer ontdekte, zonden alle machines die Blue Frog gebruikten een mail naar de spammer, in feite een botnet die een kleine DoS-aanval uitvoerde op de spammer.

* *http://blogs.guardian.co.uk/technology/2006/05/17/spammers_kick_blue_frog_into_submission.html*

• Voorlichting is belangrijk maar heeft weinig effect: het is moeilijk uit te leggen, complex en voor de consument is een infectie moeilijk te ontdekken.

• Netwerkoperators moeten technische maatregelen nemen tegen ernstige botnetaanvallen. Deze maatregelen zijn complex en beïnvloeden het gebruik; netwerkproviders moeten dan ook samenwerken met alle belanghebbenden om een limiet te stellen aan de te nemen maatregelen.

• Bots afzonderen in een "ommuurde tuin" en samenwerking met softwareleveranciers om pc's te desinfecteren lijkt effectief, maar netwerkoperators moeten een manier vinden om dat op een gebruiksvriendelijke manier te doen (de consument zo min mogelijk belasten en opt-out-mogelijkheden bieden).

CASE 3: BLOKKEREN VAN PHISHING

Probleem: ***Het doel van phishing-mails is het stelen van iemands identiteit of het frauderen tegen consumenten.***

Risico: ***Consumenten kunnen veel geld verliezen, bijvoorbeeld als hun bankgegevens online worden gestolen; het herkennen van phishing-e-mails is vaak moeilijk.***

Phishing is een van de meest kritieke en snelst groeiende problemen op het gebied van privacy- en databescherming. Het is een technisch complex fenomeen en een uitdaging om consumenten er opmerkzaam op te maken.

Nog lastiger wordt het nu phishing-e-mails en -websites steeds professioneler worden en moeilijker te onderscheiden van legitieme versies, zelfs voor deskundigen.

Voorlichting kan daardoor slechts een aanvullende rol spelen bij het beperken van schade door phishing. Naast intensievere vervolging van verantwoordelijke personen en bedrijven is een technische aanpak de belangrijkste remedie om phishing-aanvallen te blokkeren.

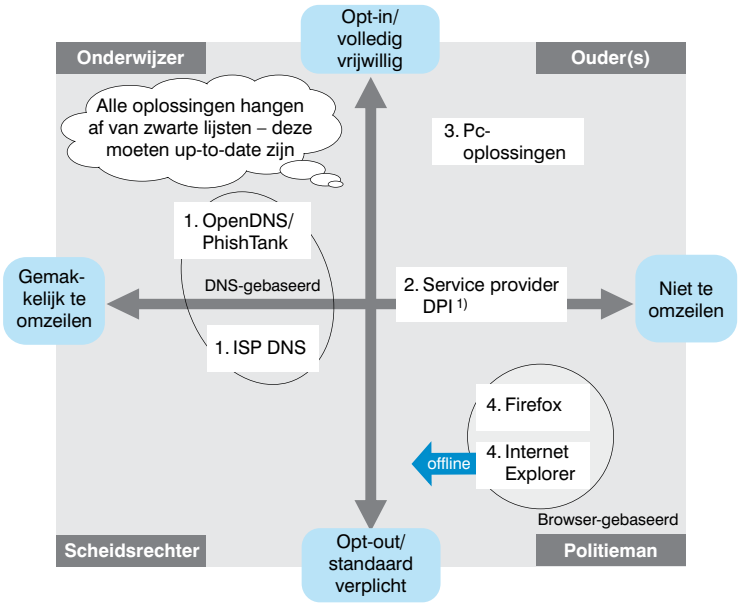
Geen enkel phishing-filter is 100 procent veilig

Zulke methodes kunnen worden besproken aan de hand van een aangepaste versie van het Digital Confidence Positioneringmodel (figuur 43). De verticale as differentieert of de gebruiker vrijwillig dient te kiezen voor een oplossing (opt-in) of dat bescherming actief is zolang hij/zij niet kiest voor opt-out. De horizontale as differentieert de mogelijkheden om de oplossing te omzeilen.

OpenDNS en PhishTank zijn voorbeelden van een op een gemeenschap gebaseerde procedure om phishing-sites te identificeren en op een zwarte lijst te plaatsen (figuur 44). Dankzij een grote gemeenschap kunnen phishing-aanvallen zeer snel ontdekt en geverifieerd worden, in minder dan twaalf uur.

Deze methode sluit aan bij de DNS-filtering (Domain Name System) en maakt gebruik van het feit dat domeinen individueel kunnen worden geblokkeerd. Het kan uitgevoerd worden bij de DNS-server van de ISP, of bij servers van derden.

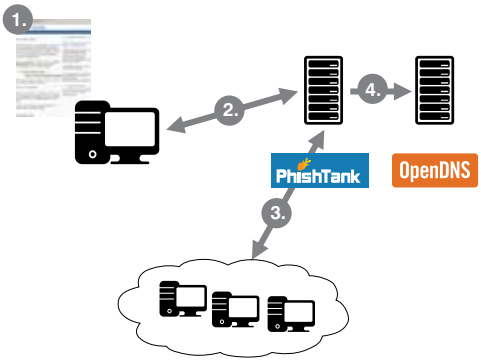
Figuur 43: *Digital Confidence positie t.a.v. blokkeren phishing*



1) Bijv. oplossingen in samenhang met reclame (Phorm)

1. DNS-gebaseerde oplossingen kunnen de toegang tot specifieke domeinen blokkeren; dit kan op de DNS-server van de service provider zijn, of op servers van derde partijen
   - Pro: Werkt voor alle applicaties (geldt niet alleen voor browser, maar ook voor mail en andere applicaties)
   - Contra: Alleen bruikbaar voor URL-gebaseerd phishing
2. Deep Packet Inspection (DPI) oplossing bij de internet provider inspecteert de content van elk pakket en kan kwaadaardig dataverkeer omleiden 1)
   - Pro: Werkt voor alle applicaties en veel phishing-aanvallen
   - Contra: Zorgen om privacy en omzeild door dataverkeer met encryptie
3. Pc-gebaseerde veiligheidsoplossingen hebben normaal ook een phishing-filter
   - Pro: Afhankelijk van de oplossing kan het alle applicaties beschermen
   - Contra: Gebruiker moet de oplossing installeren en configureren
4. Huidige browser kan URL's controleren op server- of lokale zwarte lijsten (ook heuristisch)
   - Pro: Weinig zorgen om privacy (afhankelijk van implementatie)
   - Contra: Geen bescherming in andere applicaties, bijv. mail of oudere browserversies

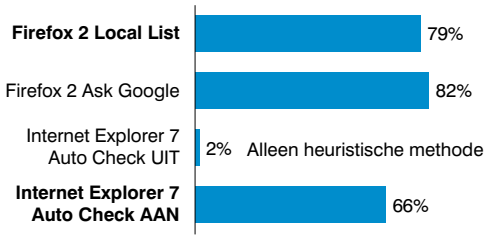
Figuur 44: *Overzicht blokkeren phishing*



1. Gebruiker ontvangt fishing-mail en gaat naar de phishing-website – **gebruiker identificeert de phishing-aanval (op basis van e-mail en website)**
2. Gebruiker stuurt URL van phishing-site naar OpenDNS/PhishTank als mogelijke bron van phishing
3. OpenDNS/PhishTank community verifieert de phishing-aanval
4. Domein wordt toegevoegd aan de zwarte lijst van PhishTank en geblokkeerd in OpenDNS
5. Verdere pogingen de link te benaderen worden geblokkeerd

Bron: OpenDNS.com, Phishtank.com

Figuur 45: *Effectiviteit van browser-gebaseerd blokkeren van phishing (2006)*



Noot: Vet-gedrukt = standaardmodus
Bron: Mozilla Foundation

Groot voordeel is dat het werkt voor alle toepassingen en dus niet alleen voor webverkeer via een internetbrowser, maar bijvoorbeeld ook voor e-mail. Deze blokkeermethode werkt evenwel alleen bij URL-gebaseerde phishing – circa 90 procent van alle phishing-aanvallen (10 procent is gebaseerd op IP-adressen en gebruikt geen domeinnamen). Andere mogelijke knelpunten zijn: bij DNS-gebaseerd blokkeren kan configuratie bij de eindgebruiker noodzakelijk zijn, afhankelijk van het soort oplossing; bij ISP-gebaseerd DNS blokkeren kan overblokkeren een groot probleem worden omdat gebruikers beperkte mogelijkheden hebben om een site te bereiken die onterecht geblokkeerd is.

Technologie staat voorop bij het blokkeren van phishing en moet op diverse niveaus ingezet worden: netwerk, pc en browser.

In de tweede plaats kunnen ISP's DPI (deep packet inspection) inzetten om phishing-aanvallen te blokkeren. Dit soort oplossingen onderzoekt de inhoud van elk pakket op het netwerk en kan kwaadaardige dataverkeer wegleiden, ook dataverkeer naar phishing-sites op een zwarte lijst. Deze methode werkt voor alle toepassingen en dus voor de meeste phishing-aanvallen. Toch kan de gebruikelijke bezorgdheid om privacy ontstaan wat betreft DPI in het algemeen: consumenten vinden wellicht dat de informatie van de serviceprovider niet transparant genoeg is, zelfs als de data veilig zijn en niet voor andere doeleinden worden gebruikt. Het gebruik van DPI tegen phishing is zeer effectief en kan alleen omzeild worden door dataverkeer te coderen (wat zelden gebeurt bij phishing-aanvallen).

Correcte zwarte lijsten zijn cruciaal: alleen phishing-pogingen die op de lijst staan kunnen geblokkeerd worden.

In de derde plaats kan de consumentencomputer centraal staan: veel pc-beveiligingsoplossingen hebben tegenwoordig een phishing-filter, zoals Norton, McAfee, Sophos en andere, vaak geleverd aan de consument door de ISP of netwerkprovider. Zulke filters zijn in veel gevallen erg effectief omdat ze, afhankelijk van de gekozen oplossing, alle toepassingen beschermen en daarmee ook een goede bescherming bieden tegen phishing. Een nadeel is dat de consument er het nodige voor moet doen: installeren, configureren en updaten. Met name het regelmatige updaten van lokale zwarte lijsten is daarbij essentieel.

Ten slotte kan phishing worden geblokkeerd middels de browser. Nieuwe browsers zoals Explorer 7 en Firefox 2 kunnen URL's nakijken op zwarte lijsten – op servers en lokaal – en zo phishing-aanvallen ontdekken en ertegen optreden. Verder kunnen er ook heuristische methodes gebruikt worden om phishing-aanvallen te ontdekken (bijvoorbeeld via patronen in URL's die vaak worden gebruikt bij phishing; deze methode heeft echter een slagingspercentage van slechts 2 procent). Voordeel van deze benadering is dat er geen privacyproblemen zijn als het blokkeren lokaal gebeurt. Zo downloadt en controleert Firefox automatisch een lijst van phishing-sites. Een beperking is dat browser-gebaseerd blokkeren niet werkt tegen phishing-aanvallen bij andere toepassingen, zoals e-mail (op dit moment slechts een kleinschalig probleem). Verder is deze methode gevoelig voor kwaadaardige software op de gebruikerscomputer, bijvoorbeeld een bot (zie hoofdstuk 3) die zwarte lijsten deactiveert of manipuleert.

Het blokkeren van phishing via de browser is zeer effectief als de meest recente versies van browsers worden gebruikt. Bij oudere browsers zoals IE 6 moeten aanvullende software van derden worden gebruikt (meestal met dezelfde zwarte lijsten).

Bij alle vier de benaderingen zijn zwarte lijsten nodig zodat het blokkeermechanisme zijn werk kan doen. Wat er op de zwarte lijst staat, is doorslaggevend voor succesvol blokkeren van phishing; als er te veel op staat ontstaat overblokkering, zodat bepaalde sites ten onrechte worden geblokkeerd (zoals een inlogpagina voor online bankieren). Als aan de andere kant niet alle gegevens op de zwarte lijst voorkomen of niet voldoende geüpdatet worden, heeft de bescherming weinig zin en kan leiden tot aansprakelijkheidsproblemen voor de provider van de zwarte lijst.

BELANGRIJKE LESSEN

Uit het bovenstaande kunnen vijf belangrijke lessen getrokken worden:

- Omdat phishing voor consumenten moeilijk te begrijpen is, heeft voorlichting waarschijnlijk niet erg veel invloed – het speelt slechts een ondergeschikte rol.

- Het blokkeren van phishing-aanvallen is een van de beste remedies – alle methodes tonen voor- en nadelen in effectiviteit, dekking (welke toepassingen zijn beschermd?), privacyzorgen en vereiste consumentenacties, die zorgvuldig afgewogen moet worden.

- Alle blokkeermethodes staan of vallen met het samenstellen en beheren van lijsten met te blokkeren phishing-sites. Er zijn tegenwoordig meerdere effectieve zwarte lijsten beschikbaar (bijvoorbeeld van Google, PhishTank) en in gebruik.

- Browsergebaseerde oplossingen zijn vandaag de dag het belangrijkst omdat ze de beste interactie met de gebruiker mogelijk maken en voorlichting kunnen geven bij een aanval. Een groot probleem zijn oudere browsers zonder bescherming – de softwaresector moet samen met ISP's nieuwere browserversies de markt op duwen.

- Methodes die (ervaren) gebruikers de mogelijkheid bieden om voor opt-out te kiezen of een blokkering te overrulen, bijvoorbeeld als content ten onrechte op de zwarte lijst staat, en de privacy van de consument (bijvoorbeeld met lokale zwarte lijsten), lijken het meest geschikt.

CASE 4: GERICHT ADVERTEREN

***Probleem:* Consumenten produceren veel data over hun gedrag tijdens het internetten en bedrijven maken hier gretig gebruik van om gerichter te kunnen adverteren.**

***Risico/kans:* Consumenten maken zich zorgen over hun privacy, maar bedrijven kunnen hun advertenties veel beter afstemmen (en daarmee hun opbrengsten verhogen).**

Web 2.0 zorgde voor de opkomst van veel diensten gebaseerd op sociaal netwerken zoals Facebook en MySpace. Veel van deze diensten braken records wat betreft toename van abonnees en gebruik – niet in de laatste plaats omdat de consument er gratis gebruik van kan maken. Toch nam hierdoor de druk op leveranciers toe om deze diensten te gelde te maken. Naar verwachting gaat adverteren, met name gericht adverteren, hierin een grote rol spelen. Onze marktanalyse toont aan dat adverteren het snelst groeiende segment van de digitale wereld zal worden (zie hoofdstuk II). Grote spelers als Google en Yahoo! zijn al gestart met het kapitaliseren van adverteren – in feite hun belangrijkste inkomstenbron. Als gevolg hiervan heeft de bedrijfstak de afgelopen tijd enkele aanzienlijke ontwikkelingen meegemaakt: in april 2007 nam Google voor $3,1 miljard DoubleClick over, een van de toonaangevende advertentiefirma's. AOL kocht Tacoda, gespecialiseerd in advertenties afgestemd op gedrag, in juli 2007 en in september 2007 kocht Yahoo! Blue Lithium, gespecialiseerd in op prestatie gebaseerde displayreclame. Ook netwerkproviders vallen steeds meer terug op businessmodellen gebaseerd op reclame om hun groeiambities te realiseren.

Op de juiste wijze gebruikt kan reclame voor zowel consumenten als de bedrijfstak een win-winsituatie opleveren. De reclame wordt relevanter en minder irritant voor consumenten, terwijl het voor adverteerders goedkoper is om zich tot een specifiek publiek te richten.

De zakelijke redenering is duidelijk: jongeren brengen steeds meer tijd door op het web. Bovendien maakt het web meer informatie over de consument toegankelijk voor de adverteerder. Waarin zijn ze geïnteresseerd? Waar wonen ze? Dergelijke informatie wordt deels openbaar gemaakt door de consument op platforms als Facebook; andere informatie kan worden verkregen door data te verzamelen over gedrag online.

Voor de meeste van deze nieuwe business-modellen is datacollectie nodig en sommige recente implementaties veroorzaakten privacyzorgen. In de Verenigde Staten bijvoorbeeld organiseerde de Federal Trade Commission (FTC) in november

2007 een congres om in breed verband "Online Behavioural Advertising" aan de orde te stellen met bijzondere nadruk op privacyproblemen en suggereerde later openlijk "Online Behavioural Advertising Principles".

Vanuit een Digital Confidence-perspectief kunnen aandrijvers en principes van gericht adverteren uiteengezet worden in een aangepaste versie van het generieke Digital Confidence Positionering-model (figuur 46). De horizontale as differentieert of het gericht adverteren website-/toepassinggedreven is (door internetspelers zoals sociale netwerken), of netwerkgedreven (door kabeloperators of ISP's). De verticale as differentieert de mate waarin de gebruiker controle heeft over zijn of haar data en of ze worden gebruikt voor dit soort adverteren, met mogelijkheden van "opt-in" (beslissing ligt volledig bij de gebruiker) tot "geen opt-out" (data worden gebruikt zonder inspraak van de gebruiker.

85 procent van de gebruikers is ertegen dat websites advertenties tonen op basis van websites die ze eerder bezochten.

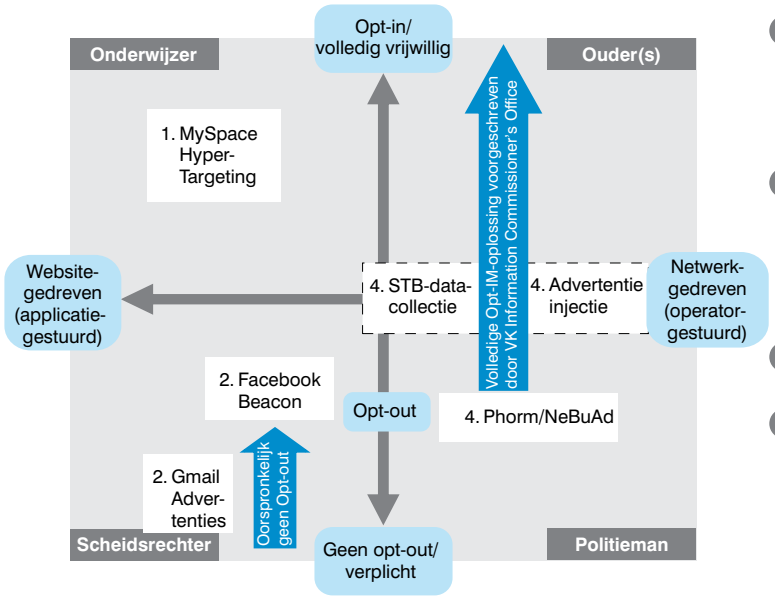
Er zijn vier duidelijke voorbeelden hoe gericht adverteren geïmplementeerd kan worden. MySpace test een oplossing die specifiek opt-in zou zijn. Facebook daarentegen startte in 2007 met Beacon, een oplossing aanvankelijk geïmplementeerd zonder gebruikerstoestemming. Pas na een grote publieke discussie werd dit veranderd in een opt-out-oplossing. Een voorbeeld van succesvol gericht adverteren is Gmail: Google biedt een gratis e-mailservice, maar analyseert de content van de berichten om gerichte advertenties in de interface te tonen. Deze advertenties zijn een integraal onderdeel van Google's e-mailservice en gebruikers hebben te accepteren dat de getoonde advertenties afhangen van hun e-mail – gezien het succes van Gmail lijken ze dit geen probleem te vinden. Bij de introductie van Gmail in 2004 leidde dit echter wel tot forse controverses over privacy, met name het ongelimiteerd opslaan van gegevens en het feit dat e-mails van niet-Gmail abonnees naar Gmail abonnees zonder hun toestemming werden geanalyseerd.

Meerdere partners stopten hun medewerking toen ze zich realiseerden dat Facebook's Beacon geen opt-in-oplossing is.

De MySpace HyperTargeting-oplossing rangschikt gebruikers op basis van hun interesses zoals die op het publieke profiel staan (meer dan 100 categorieën). Hieruit kunnen adverteerders een keuze maken voor hun campagnes. In de eerste tests bereikte MySpace een toename van 300 procent in "doorklikken" – drie keer zo veel consumenten klikten op een advertentie – en 50 procent extra kosten voor duizenden impressies of "cost per mille" (CPM) CPM is de standaard voor het betalen voor adverteren op basis van het aantal consumenten dat een advertentie bekijkt. Hoewel MySpace tot nog toe alleen test, zijn er al heftige discussies over privacy. Gezien het feit dat oplossing opt-in zal worden, lijkt MySpace oog te hebben voor de bezorgdheid van zijn gebruikers.

Facebook's Beacon daarentegen werd bij de lancering in november 2007 met 44 partnersites ingezet voor alle gebruikers zonder toestemming vooraf. Het integreerde Facebook in de

Figuur 46: *Digital Confidence positie t.a.v. gericht adverteren*



1. MySpace's HyperTargeting categoriseert gebruikers op basis van hun aangegeven interesses en toont ze hierop gebaseerde reclame
   - Adverteerders kunnen categorieën kiezen
   - Momenteel alleen in testfase, maar toch al zorgen om privacy
2. Facebook Beacon integreert Facebook met andere sites (acties op andere sites worden doorgestuurd naar Facebook)
   - Aanvankelijk als vervolg op 'Facebook Stories', maar kan worden gebruikt voor gericht adverteren
   - Extreme zorgen om privacy na introductie, inclusief rechtszaken tegen partnersites ('Harris vs. Blockbuster')
3. Google Mail past reclame aan aan de content van e-mails ('automated content recognition')
4. Service provide-gebaseerde oplossingen analyseren alle webactiviteiten van gebruikers ('advertentie serving' voor partnersites of 'advertentie injectie' in alle sites [1])
   Privacyzorgen doordat alle dataverkeer wordt onderzocht om profielen af te leiden
   Na test BT zonder toestemming van consumenten, eiste het ICO (VK) Phorm-implementaties naar Brits recht

1) Huidige oplossingen richten zich op advertentie serving

partnersites en maakte daarmee het op grote schaal uitwisselen van datacollecties en profielen mogelijk, zolang een gebruiker ingelogd was op Facebook. Aanvankelijk was het bedoeld om Facebook-stories beter te kunnen bekijken ("je vriend bekeek video xxx op Joost"), maar gericht adverteren is ook mogelijk. Na de introductie ontstonden ernstige privacyzorgen, inclusief rechtszaken tegen deelnemende sites. Als reactie introduceerde Facebook al in december 2007 een opt-out-mogelijkheid.

In het Gmail-voorbeeld komen de zorgen openlijk aan het licht. Google legt op zijn website op een transparante manier uit dat gebruikers meer voordeel hebben van gericht adverteren bij e-mails dan van niet-gericht adverteren: "Google is van mening dat het tonen van voor gebruikers relevante advertenties meer waarde biedt dan zomaar pop-ups laten zien of ongerichte bannerreclame." De Gmail-oplossing lijkt ook minder controversieel; gebruikers melden dat ze de advertenties nuttig vinden en de data worden beperkt gebruikt – alleen voor advertenties aan de gebruiker in kwestie en alleen binnen de Gmail-toepassing.

Phorm en NebuAd leveren Netwerk-gebaseerde oplossingen voor gericht adverteren, met de mogelijkheid al het surfgedrag van gebruikers te analyseren en advertenties gericht te laten zien. Phorm wordt binnenkort getest door grote netwerkproviders, zoals BT en Virgin in Groot-Brittannië. Phorm gebruikt DPI om surfgedrag te analyseren; alle dataverkeer wordt geïnspecteerd om er profielen van af te leiden.

Deze zeer geavanceerde capaciteiten van DPI om het internet te monitoren, zelfs als de data geanonimiseerd zijn, hebben de aandacht van regelgevers sterker gericht op privacyrisico's. De inzet van deze diensten heeft in sommige markten geleid tot aanzienlijke media-aandacht en gebruikerskritiek, zeker op de manier waarop netwerkoperators deze technieken (proberen te) testen. Zo startte BT een pre-trial van Phorm-gebaseerd gericht adverteren zonder de betrokken consumenten te informeren. Dit leidde tot tussenkomst van de Britse Information Commissioner's Office (ICO), die verklaarde dat bij de trial betrokken consumenten op de hoogte moesten worden gesteld van de technologie en hun toestemming moesten geven door "opting in" voor de trial, met de mogelijkheid van "opting out" daarna.

Charter Communications, de op drie na grootste kabeloperator in de Verenigde Staten, schoof zijn trial voor gericht adverteren binnen een maand op de lange baan. In de Vraag & Antwoord-sectie van de website waren ze er redelijk open over, maar gebruikers waren niet overtuigd van de beloofde voordelen – een "betere browserervaring". Ook vond men het gebruik van DPI te ingrijpend. Garanties dat persoonlijke profielen veilig waren, werden eveneens in twijfel getrokken. Ten slotte werd Charter's opt-out-oplossing omslachtig gevonden. Gebruikers moesten een formulier invullen en een cookie accepteren. Het verwijderen van cookies of het overschakelen naar een andere browser maakte evenwel gericht adverteren weer mogelijk, totdat het opt-out-formulier nogmaals was ingevuld.

Naast oplossingen als Phorm kan op het netwerk gebaseerd gericht adverteren ook plaatsvinden via de set-topbox en als "ad-injectie". Hierdoor kunnen community-achtige features hun weg vinden naar het digitale TV-platform (bijvoorbeeld populariteitsratings) en cross-platform promoties. Gericht adverteren is ook mogelijk, aangezien de set top box-interface interactief advertenties kan tonen, bijvoorbeeld om VoD-aanbiedingen te promoten gebaseerd op kijkgedrag ("U heeft tien documentaires bekeken over de Afrikaanse dierenwereld; wilt u een documentaire over leeuwen downloaden?"). De set-topbox-methode registreert data over het "zap"gedrag en bekeken tv-programma's.

BELANGRIJKE LESSEN

Uit het bovenstaande kunnen zes belangrijke lessen getrokken worden:

- Gericht adverteren is duidelijk in opkomst door een aantal factoren: breedband als massafenomeen, verspreiding van zeer geavanceerde technologieën om het internet te monitoren en de behoefte aan nieuwe businessmodellen van internetspelers en netwerkproviders om nieuwe Web 2.0-services en -platforms te gelde te maken.

- Gericht adverteren is het sleutelwoord voor internetnet- en netwerkproviders om diensten en innovaties van de volgende generatie te financieren en met name om veel Web 2.0-services en -toepassingen te gelde te maken – wat een meerwaarde voor de consument kan zijn indien op de juiste manier gedaan (bijvoorbeeld Gmail).

- Sites voor sociaal netwerken leveren een veelheid aan data en zijn dan ook zeer geschikt voor gericht adverteren; netwerkproviders beginnen deze mogelijkheden nog maar net te overwegen.

- Pogingen tot gericht adverteren met DPI-technologie zijn in de media en onder het publiek veelbesproken en hebben bezorgdheid over de privacy en in veel gevallen weerzin gewekt.

• Aanvaarding door de gebruiker vergt meer dan naleving van de privacywegeving. Doorzichtigheid naar de gebruikers over mogelijke gerichte reclame is essentieel. Ook belangrijk is het benadrukken van de toegevoegde waarde voor de consument, hen overtuigen van het nut en toegevoegde waarde voor henzelf.

• Wat betreft de feitelijke implementatie door netwerkoperators is al duidelijk geworden dat niet-transparante praktijken kunnen leiden tot gereguleerde opt-in-verplichtingen. Makkelijk te gebruiken opt-out hulpmiddelen met transparante communicatie naar gebruikers wordt wellicht aanvaard, met name in combinatie met een echte (gratis?) meerwaarde zoals het Gmail-voorbeeld laat zien.

CASE 5: BLOKKEREN VAN KINDERPORNOGRAFIE

Probleem: ***Toegang blokkeren tot websites met kinderpornografie (enkele duizenden sites).***
Risico: ***Gering reëel risico om onbedoeld op een site met kinderpornografie terecht te komen, maar vindbaar na zoeken; ernstige impact op het leven van slachtoffers.***

Kinderpornografie is in de meeste landen bij de wet verboden (alleen afwijkende definities voor "kind" en "minderjarige": tussen veertien en achttien jaar in de meeste landen). Toch zijn er duizenden sites op het internet met dergelijke content.

Bestrijding van kinderpornografie benadrukt de vervolging van personen die verantwoordelijk zijn voor het bestaan van kinderpornografie: gebruikers/consumenten van kinderpornografie enerzijds en leveranciers van dergelijk materiaal anderzijds. Vervolging van betrokken personen of bedrijven is uitsluitend een taak voor wetshandhavende instanties, die hulp kunnen eisen van andere belanghebbenden (bijvoorbeeld netwerkproviders) waar nodig en wettelijk uitvoerbaar. De autoriteiten doen steeds meer op dit gebied: in mei 2008 bedeelde de Senaat van de Verenigde Staten een budget toe van $1 miljard gedurende de komende acht jaar om op grote schaal kinderpornografie te bestrijden.

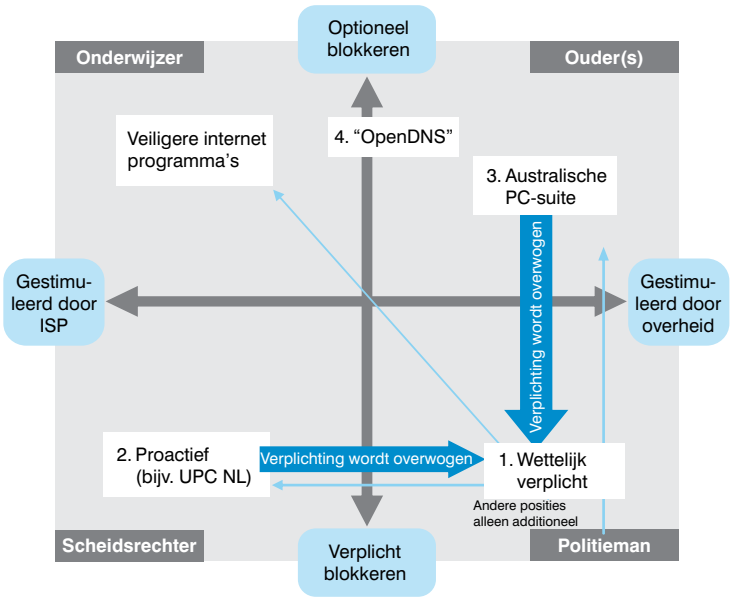
*In de Verenigde Staten worden elk jaar meer dan 1.500 peronen gearresteerd vanwege het bezit van internetgerelateerde content met kinderpornografie. De meerderheid hiervan bezit meerdere honderden foto's van kinderen tussen zes en twaalf jaar.**

Aan de andere kant is het voorkomen dat internetgebruikers ongewild kinderpornografie zien een taak voor met name de netwerkproviders. Dit is echter moeilijker dan het lijkt, omdat het vele facetten kent en zeer controversieel is: blokkeren stelt de verantwoordelijke instantie bloot aan kritiek over censuur en aansprakelijkheidsclaims en waterdicht blokkeren is technisch moeilijk aangezien alle beschikbare technieken te omzeilen zijn.

Huidige wetgeving bestrijkt niet alle nieuwe internetgerelateerde probleemgebieden die te maken hebben met sexueel misbruik

* *National Centre for Missing & Exploited Children*

Figuur 47: *Digital Confidence positie t.a.v. blokkeren kinderpornografie*



1. Standaard ISP-positie: content alleen blokkeren indien wettelijk voorgeschreven
   - Pro: Basisbescherming gegarandeerd
   - Contra: Geen additionele bescherming mogelijk
2. ISPs initiëren proactief het blokkeren van programma's zonder daartoe wettelijk verplicht te zijn
   - Pro: Voorkomt onbedoelde/toevallige toegang
   - Contra: Censuur dreigt als zwarte lijsten door derden verder worden uitgebreid dan hun eigenlijke doel
3. De Australische overheid ontwikkelde een pc-gebaseerde oplossing voor ouders
   - Pro: Door iedereen te gebruiken
   - Contra: Speciale expertise nodig om te installeren en configureren
4. Oplossingen van het type "OpenDNS" zijn branchegestuurd en stellen gebruikers in staat te kiezen welke categorieën geblokkeerd moeten worden
   - Pro: ISP niet verantwoordelijk voor geselecteerde content
   - Contra: Geen uniform beschermingsniveau – afhankelijk van individuele actie en voorkeuren

Eén probleem is dat kinderpornografie gedefinieerd moet worden om het te criminaliseren en blokkeren: de grens tussen pornografie en kunst is soms vaag. Bovendien moeten de criteria hard gemaakt kunnen worden: of een jongere die in een pornografische context wordt getoond al dan niet moet worden beschermd – in de meeste landen is een bepaalde leeftijdsgrens doorslaggevend – is (bijna) onmogelijk vast te stellen. Bovendien zorgen digitaal bewerkte en gemanipuleerde foto's voor een nieuw (juridisch) probleem dat nog niet bestond toen de meeste wetten werden opgesteld.

Methodes om kinderpornografie te blokkeren kunnen bezien worden aan de hand van een aangepaste versie van het Digital Confidence Positioneringmodel. De verticale as differentieert of het blokkeren optioneel is (naar keuze van de consument), zelfopgelegd (bepaald door de netwerkoperator) of verplicht. De horizontale as differentieert of de netwerkoperators dan wel de regelgever de drijvende kracht achter deze activiteit is.

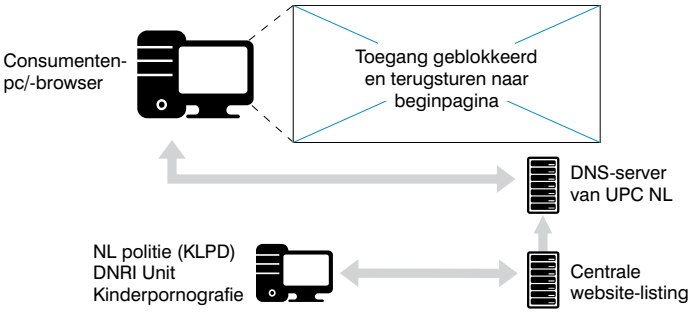
Tot dusver is, naast het naleven van het juridisch verplichte blokkeren van sites, de meest gebruikte methode het op eigen initiatief filteren van kinderpornografie. Dit is gebaseerd op onafhankelijke, door derden samengestelde en geverifieerde lijsten van juridisch verboden sites. ISP's zijn meestal terughoudend met filteren, omdat ze "slechts een doorgeefluik" zijn en het niet aan hen is om zich met internetvrijheid te bemoeien. Bovendien willen ze juridische aansprakelijkheid voorkomen mocht er ongewild legale content geblokkeerd worden. Indien filtering wordt toegepast, vrijwillig dan wel wettelijk verplicht, zijn onafhankelijke wettelijke controles vereist om vast te stellen dat de te filteren content daadwerkelijk onrechtmatig is onder de geldende wetgeving.

Technische experts (zelfs kinderen) kunnen de meeste pc-filters gemakkelijk omzeilen.

Een goed voorbeeld van een proactieve ISP is het initiatief van het Nederlandse UPC begin 2007 om kinderpornografie te filteren. UPC werkt samen met het Nederlandse ministerie van Justitie en de Nederlandse politie die een zwarte lijst hebben opgesteld van meer dan 3.000 websites met kinderpornografie en de toegang bemoeilijken door een pagina te tonen met de tekst "U probeert toegang te krijgen tot een website op de zwarte lijst". Met deze oplossing werd duizenden keren per maand voorkomen dat ongewild een kinderpornosite werd bezocht.

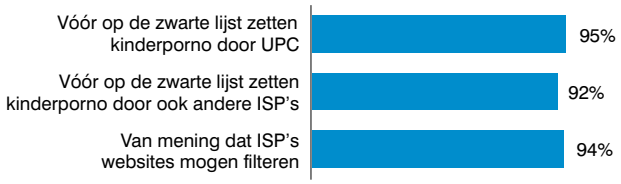
Het publiek reageerde hier zeer positief op.

Figuur 48: *Blokkeren kinderpornografie – technische implementatie*



Noot: Technische oplossing gesimplificeerd
Bron: UPC

Figuur 49: *Blokkeren kinderpornografie – publieke opinie*



Bron: NSS Interviews (n = 600)

Een speciale enquete gaf aan dat 95 procent van de consumenten voorstander was van het op de zwarte lijst zetten van kinderpornografie en 94 procent voorstander van het filteren van ongewenste content in het algemeen door netwerkoperators. Dit laatste percentage lijkt erg hoog, maar werd wellicht beïnvloed door het feit dat de vraag gesteld werd in een context van kinderpornografie en niet in een neutrale context. Daarnaast reageerde ook de pers grotendeels (63 procent) positief op het filteren. Desondanks werd er in het Nederlandse parlement bezorgdheid geuit over de doeltreffendheid van DNS-filteren en het feit dat niet alle ISP's filters gebruikten. Het parlement vroeg de regering om de mogelijkheid tot verplicht filteren bij Nederlandse ISP's te onderzoeken.

Het grote voordeel van vrijwillige ISP-initiatieven is dat ze uitgebreide bescherming kunnen bieden als toonaangevende instanties hun krachten bundelen om trage of onvolledige wetgeving te compenseren. Het probleem voor netwerkproviders en ISP's is dat ze zichzelf blootstellen aan verzoeken om het filteren uit te breiden – een "hellend vlak" richting censuur en aansprakelijkheidsproblemen. Voorbeelden die dit illustreren: in juli 2007 wilde de Zweedse politie's werelds grootste BitTorrent-tracker, The Pirate Bay, toevoegen aan een zwarte lijst met kinderpornosites. In Denemarken beval de rechtbank om een DNS-gebaseerde zwarte lijst van kinderpornosites uit te breiden met populaire

sites om muziek te downloaden (het Russische AllofMP3.com en opnieuw The Pirate Bay), hetgeen de verspreiding van informatie over het omzeilen van dergelijke lijsten bevorderde, waardoor de doeltreffendheid van originele filter werd ondermijnd.

In Australië zien we een andere aanpak: sinds 2007 overweegt de Australische regering een tweesporige aanpak, waarbij enerzijds ISP's verplicht zouden worden om te filteren. Tot dusver is dit deel van het project gestrand na een aantal mislukte pogingen waarbij filteroplossingen niet schaalbaar bleken voor grote ISP's. Bovendien is er veel politieke controverse rond het soort en de aard van content op de zwarte lijst, die wordt bijgehouden door de ACMA (Australian Communications and Media Authority).

Anderzijds ontwikkelde de regering NetAlert, een software programma bedoeld voor "Protecting Australian Families Online", waarin opgenomen het blokkeren van content met kinderpornografie. Dit is een personal-computergebaseerde oplossing om content te filteren, vergelijkbaar met vele commerciële oplossingen. Deze aanpak stelt de keus en verantwoordelijkheid van de consument centraal, maar vereist ook enig initiatief en een zekere expertise van consumenten om het te laten werken. Aangezien veel gebruikers niet bijzonder technisch zijn, is oplossing lastig inzetbaar (er zijn niet meer dan 100 installaties genoteerd na de aanvankelijke opzet) en door meer ervaren gebruikers gemakkelijk te omzeilen. Zo werd gemeld dat een tiener dit filter ter waarde van AU$84 miljoen binnen een halfuur wist te omzeilen.

Zoals blijkt uit het Australische voorbeeld biedt geen enkele filtermethode een 100 procent zekere oplossing tegen bewuste omzeiling. Bovendien speelt bij elke vorm van filteren de kwaliteit van de lijst met illegale content een doorslaggevende rol. Die moet goed beheerd, geactualiseerd en toegepast worden. Verder is het van belang dat de illegale content ook snel verwijderd wordt. Volgens "notice and takedown"-schema's bleven sites met kinderpornografie gemiddeld 30 dagen online nadat ze voor het eerst gemeld werden. Nationale hotlines staan voor de uitdaging om internationale wetshandhavers (via Interpol of Eurojust) snel actie te doen ondernemen om te zorgen dat content snel wordt verwijderd door de hostingproviders nadat de hotlines ze hebben gewaarschuwd voor illegale content in hun rechtsgebied. Volgens de Britse Internet Watch Foundation was 2 procent van commerciële sites met kinderpornografie wereldwijd een jaar na constatering nog steeds actief.

Filteren van content ter bestrijding van content met seksueel misbruik van kinderen neigt voor ISP's en netwerkproviders al snel naar censuur.

Het ontbreken van een 100 procent zekere oplossing, de variabele kwaliteit van zwarte lijsten en variaties in wetshandhaving zijn evenzoveel factoren waarmee rekening moet worden gehouden bij het vaststellen van de proportionaliteit van verplicht filteren door ISP's.

Ten slotte bestaat de mogelijkheid om het blokkeren van kinderpornografie geheel over te laten aan de consument. Een schoolvoorbeeld van deze aanpak is de implementatie van OpenDNS. OpenDNS[7)] is een gratis DNS-server die gebruikers de mogelijkheid geeft om bepaalde categorieën sites te blokkeren in een webinterface. De DNS-server stuurt gebruikers door naar een landingspagina als zij toegang proberen te krijgen tot geblokkeerde content. De beslissing aan de gebruiker overlaten heeft grote voordelen: consumenten kiezen zelf wat ze zien of blokkeren (uiteraard afgezien van wettelijke verplichte blokkeringen) waardoor discussies over censuur of aansprakelijkheid verdwijnen. Daarnaast kan een eenvoudige, Netwerk-gebaseerde oplossing gemakkelijk worden toegepast

Bestaande zwarte lijsten en medewerking door NGO's

In het VK hebben ISP's filteren op URL-basis geïntroduceerd voor 96 procent van particuliere breedbandklanten. De lijst van URL's wordt geleverd door de Internet Watch Foundation (IWF) van de VK en omvat duizenden URL's zowel als gemiddeld 250 tot 300 domeinnamen van commerciële websites die beelden en video's van het misbruiken van kinderen te koop aanbieden. Zes mensen verwerken bij de IWF Hotline meldingen, keuren en sporen content op, en houden de IWF URL-lijst bij. De IWF werkt de lijst twee maal daags bij en eist van de aangesloten ISP's dat zij hun filters dienovereenkomstig actualiseren, ten minste een maal per 24 uur. IWF deelt de lijst met buitenlandse hotlines (tot dusver met de Deense, Australische en Koreaanse hotlines) op basis van een overeenkomst dat de lijst wettig beoordeeld wordt om naleving van de wetgeving in de respectievelijke jurisdicties te garanderen.

In de VS zijn Verizon, Sprint, Time Warner Cable, AT&T, en AOL in juni/juli 2008 overeengekomen om de toegang tot websites en newsgroups die beelden van kindermisbruik verspreiden, te blokkeren.

7) Noot: OpenDNS is te vinden op http:// www.opendns.com. We verwijzen in dit document meermaals naar OpenDNS als voorbeeld, omdat het een gratis oplossing is die alle lezers van dit document kunnen testen

De bedrijven wordt verzocht te vergelijken met een register van expliciete sites bijgehouden door het Centre for Missing and Exploited Children (centrum voor vermiste en misbruikte kinderen). Het streven van de overeenkomst is om het uitermate moeilijk te maken om dit materiaal online te vinden of te verspreiden, al is bekend dat toegang niet volkomen geëlimineerd kan worden omdat sommige derden betaalde abonnementen verkopen, waarmee klanten zelf toegang verkrijgen tot newsgroups en zelfs hun ISP's verhinderen om hun activiteiten te zien. Een verzameling van rond de 11.400 illegale beelden werd opgesteld waarmee onderzoekers tienduizenden online bestanden tegelijk kunnen filteren. Het systeem is gebaseerd op het gebruik van beelden met unieke "hash values" – een soort digitale vingerafdruk – voor het identificeren van illegale beelden die vervolgens kunnen worden gebruikt om naar hetzelfde beeld te zoeken waar het dan ook verschijnt op het web.

www.nystopchildporn.com, een initiatief van de State Attorney General van New York, Andrew Cuomo, vermeldt welke ISP's overeenkomsten hebben ondertekend over het uitroeien van toegang tot kinderporno via hun servers.

door de "gemiddelde gebruiker". Vergeleken met proxyservers en desktop-gebaseerde systemen vergt een DNS-server-gebaseerde oplossing slechts weinig configuratie. Om het beoogde resultaat te bereiken moeten consumenten evenwel beschikken over geschikte, makkelijk bruikbare hulmiddelen en de juiste informatie en de te blokkeren content dient op de juiste wijze beheerd te worden, liefst op sectorniveau.

BELANGRIJKE LESSEN

Uit het bovenstaande kunnen acht belangrijke lessen worden getrokken:

• Het blokkeren van kinderpornografie wordt in het algemeen gezien als moreel gerechtvaardigd en dus gewenst – over het blokkeren van andere "ongewenste" sites (bijvoorbeeld racistische sites of sites voor bomfabricage) is men minder unaniem, met name met het oog op vrijheid van meningsuiting.

• Zwarte lijsten toepassen op andere content, zoals illegale muzieksites, die populair zijn en lang niet zo sterk worden afgekeurd als kinderpornografie, werkt contraproductief omdat het aanzet tot het verspreiden van informatie over het omzeilen van filters.

• Foutloze tenuitvoerlegging is zowel technisch als juridisch lastig omdat wetgeving verschilt ten aanzien van de definitie van illegale kinderpornografische content. Internationale verdragen om een eenduidige wettelijke grond te creëren – zoals het Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik uit 2007 – zijn niet in alle lidstaten geïmplementeerd.

• Om sites die op zwarte lijsten staan snel te kunnen verwijderen is een internationaal georganiseerde aanpak van wetstoepassing noodzakelijk.

• Verwachtingen over de effectiviteit van filteren moeten realistisch zijn. Geen enkel filter is 100 procent doeltreffend. Netwerk-gebaseerd filteren kan alleen helpen om onbedoelde toegang tot kinderpornografie te voorkomen. Dit is een belangrijke afweging ten aanzien van de proportionaliteit van wettelijk verplichte filtering.

• Het blokkeren van kinderpornografie leidt tot grote controverses rond censuur, aansprakelijkheid en grensoverschrijdende verschillen.

• Uit het bovenstaande vloeien twee belangrijke remedies voort:

– In landen waar geen sprake is van adequate, onafhankelijke samenstelling van lijsten: stel de consument in staat zichzelf te helpen (stimuleer in brede kring oplossingen van het Open DNS-type) en informeer de consument over de functies en werking van zulke oplossingen.

– In landen waar sprake is van steun van derden bij het opstellen van lijsten moet de bedrijfstak beslissen over de mate waarin filteren vrijwillig wordt toegepast. Begin met DNS-gebaseerd filteren als de minst opdringerige vorm van interventie of ga over tot het volgende niveau van URL-gebaseerd filteren alleen als adequate en wettelijk geverifieerde lijsten bestaan.

• Om te voorkomen dat filteren zich uitbreidt naar andere gebieden dan het bestrijden van kinderpornografie, zouden instanties die verantwoordelijk zijn voor de lijsten idealiter onafhankelijk moeten opereren van juridische autoriteiten zoals de politie. De Britse Internet

Watch Foundation is een goed voorbeeld van een dergelijke organisatie.

CASE 6: SOCIAAL NETWERKEN/ INTERNETEDUCATIE

Probleem: ***Kinderen en jeugd zijn zich niet bewust van de risico's van online-interactie (bijvoorbeeld bij sociale netwerken): uitlokking, grooming, etc.***

Risico: ***Door de grote anonimiteit van het internet is er meer risico dan in het echte leven (de meeste kinderen weten wel dat ze op straat niet met vreemden moeten praten, maar wat is een vreemde op het internet?).***

Naast het blokkeren van kinderpornografie (en mogelijk schadelijkere en nog ongewenstere content) is er een tweede manier om minderjarigen te beschermen: hen voorlichten over mogelijkheden en bedreigingen op het internet, zodat minderjarigen zelf kunnen bijdragen aan hun bescherming.

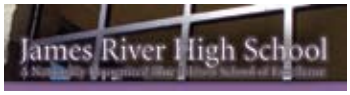
Sociale interactie dankzij het internet heeft, parallel aan de snelle groei ervan, tot problemen geleid die vroeger nauwelijks bekend waren: pesten, grooming en uitlokking, alsmede het willekeurig publiceren van gegevens.

Onvoorbereid de helpende hand toesteken kan te veel gevraagd zijn van zowel ouders als scholen, die de "typische opvoedingsprotagonisten" zijn. Hoe meer moeite ze hebben met de digitale wereld, des te groter de noodzaak voor het volgende:

1. Ouders en scholen moeten in staat worden gesteld (of zichzelf in staat stellen) om te voldoen aan de verwachtingen op het gebied van voorlichting.

2. Andere instanties – ISP's, netwerkoperators en internetbedrijven zoals platforms voor sociaal netwerken – moeten bijdragen aan de voorlichting in brede zin.

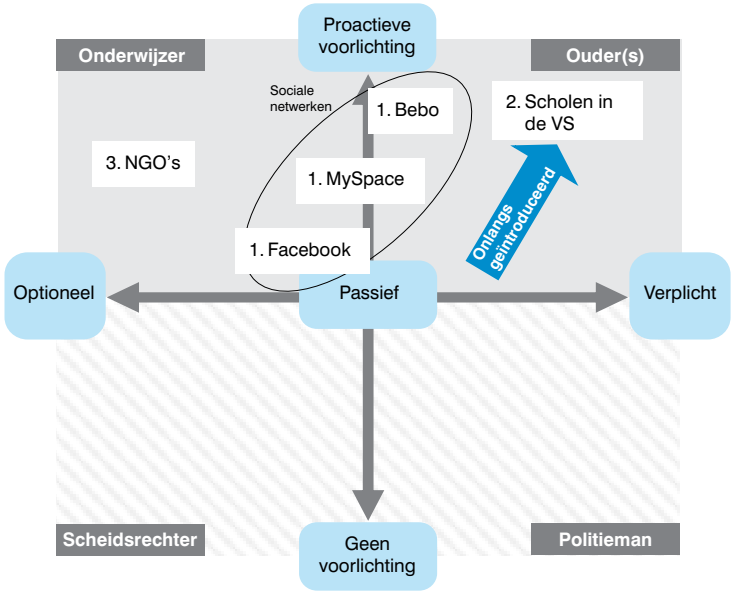
Manieren om dergelijke voorlichting aan te pakken kunnen worden besproken aan de hand van een aangepaste versie van het Digital Confidence Positioneringmodel (figuur 50). De verticale as differentieert de mate van activiteit, waarbij de onderste helft theoretisch wordt, aangezien "geen voorlichting" geen geldige optie is. De horizontale as differentieert de individuele inbreng in dergelijke educatie, dat wil zeggen of de aanpak van voorlichting een vrijblijvende optie of een verplichte taak is.



Internetbelanghebbenden kunnen kinderen en ouders van diverse voorlichtingsmaatregelen voorzien.

In de eerste plaats blijken sites voor sociaal

Figuur 50: *Digital Confidence positie t.a.v. sociaal netwerken/online educatie*



1. Sites voor sociaal netwerken lichten hun gebruikers in over de bedreigingen en gevaren van het delen van data en het te "open en vriendschappelijk zijn"
   - Bebo zeer gericht op minderjarigen en interactief, met zeer beperkende standaardinstellingen
   - MySpace en Facebook minder gericht op minderjarigen en minder beperkend
2. Scholen in de VS starten speciale cursussen over internet en sociale netwerken
   - Focus op risico's in sociale netwerken (bijv. lastigvallen)
   - Bijvoorbeeld in Virgina als verplichte cursus
   - Ondersteund door NGO's die materiaal ontwikkelen (bijv. Web Wise Kids)
3. NGO's zoals ConnectSafely geven kinderen, ouders en onderwijzers informatie over het internet

Figuur 51: *Kennisdeling over sociale netwerken door Bebo*

- Informatievideo over sociale netwerken gericht op de gevaren voor de doelgroep-kinderen (komische video's)
- Schriftelijk informatiemateriaal voor onderwijzers en ouders
- Samenwerking met relevante NGO's om materialen te ontwikkelen

netwerken duidelijk toegewijd aan gebruikersvoorlichting, zoals duidelijk wordt uit de voorbeelden Bebo, MySpace en Facebook. Ze nemen min of meer dezelfde, gematigde positie in op het vlak "verplicht-optioneel", maar ze verschillen zeer duidelijk in proactiviteit.

Bebo is sterk gericht op minderjarigen en stelt zich dan ook duidelijk proactief op waar het gaat om gebruikerseducatie. Zo is er een voorlichtingsvideo over de gevaren van sociaal netwerken met een stripachtige, vermakelijke en intuïtieve stijl speciaal voor kinderen. Bovendien biedt Bebo schriftelijke voorlichtingsmateriaal voor onderwijzers en ouders, en werkt samen met een aantal NGO's bij de ontwikkeling ervan.

Sociaal netwerken vereist een volgende stap in gebruikersvoorlichting – alle spelers moeten het belang ervan inzien en met effectieve oplossingen komen.

Facebook stelt zich gematigder op wat betreft gebruikersvoorlichting, waarschijnlijk omdat de doelgroep uit meer ervaren en oudere gebruikers bestaat. Op de site staat uitleg over vijf veiligheidstips en veelgestelde vragen voor gebruikers, maar ook specifiek voor ouders, met name over klachtenbehandeling.

Ouders verwachten in de eerste plaats van scholen dat ze verantwoordelijk zijn voor interneteducatie

In de tweede plaats zijn scholen in de Verenigde Staten onlangs gestart met speciale lessen met voorlichting over internet en sociaal netwerken. In Virginia zijn lessen in internetveiligheid al verplicht op middelbare scholen.

Men richt zich met name op de gevaren van sociaal netwerken, vooral intimidatie en uitlokking. De lessen zijn gebaseerd op materiaal ontwikkeld door de NGO Web Wise Kids.

In de derde plaats houden veel NGO's zich bezig met voorlichting over internet en sociaal netwerken, vaak duidelijk gericht op minderjarigen.

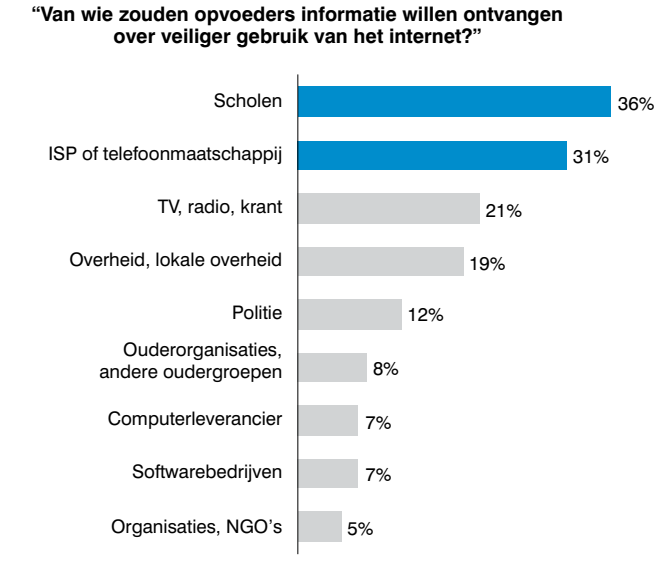
Sociaal netwerken komt steeds vaker voor en Web 2.0 speelt daar op in: ConnectSafely is een forum met als enige doel "praten over veilige sociale omgang op het vaste en mobiele web"

Web Wise Kids is een grote Amerikaanse NGO die zich bezighoudt met veiligheid op het internet. Het heeft diverse digitale, op kinderen gerichte spellen ontwikkeld die ingaan op best practices voor gedrag in het algemeen en op kwesties als uitlokking, kwaadwillige aanvallen en onrechtmatig downloaden in het bijzonder. Ook wordt aan scholen hulp geboden door "off-line" lesmateriaal ter beschikking te stellen en zich persoonlijk te richten tot de diverse belanghebbenden: van ouders en onderwijzers tot wetshandhavers en de minderjarigen zelf.

Het Europese Insafe is een netwerk van nationale knooppunten dat bewustzijn van veiligheid op het internet coördineert. Een voorbeeld daarvan is de Family e-Safety-kit, begin 2008 gepubliceerd in Europese landen. Het behandelt belangrijke veiligheidskwesties om samen met kinderen te lezen.

Ondanks deze positieve voorbeelden is er nog een lange weg te gaan om gelijke tred te houden met de snelle groei van internetgebruik door minderjarigen en met name het sociaal netwerken. Er zijn dus al veel goede initiatieven.

Figuur 52: *Informatiekanalen ouder(s) (VK, 2006)*



Bron: Eurobarometer

Maar er moet meer centraal georganiseerde actie ondernomen worden, zodat belanghebbenden gezamenlijk de geleerde lessen, best practice en succesvolle voorlichtingsmaterialen delen, hetgeen ook financieel voordeel kan opleveren.

Vooral introductie in de formele educatieve systemen is nog maar net begonnen. Enquêtes wijzen uit dat ouders de school als belangrijkste informatiebron zien over veiligheid op het internet. Interessant genoeg staat de "ISP of telefoonmaatschappij" met slechts weinig afstand op de tweede plaats. Hoewel slechts zeven procent de softwarefabrikanten noemde, zou integratie van voorlichtingsmaatregelen in de gebruikersinterface (het besturingssysteem en browsers) een logische stap zijn om meer gebruikers actief te bereiken.

*"Een internetprovider die vrijwillig zijn copyrightimmuniteit opgeeft is als een astronaut op de maan die zijn ruimtepak uittrekt." **

BELANGRIJKE LESSEN

Zes belangrijke lessen komen uit het bovenstaande naar voren:

- Minderjarigen voorzien van informatie over de mogelijkheden en gevaren van het internet in het algemeen en van sociaal netwerken in het bijzonder wordt steeds belangrijker.

- Sociale netwerken proberen hun gebruikers te informeren, maar op vrijwillige basis en naar eigen inzicht – de maatschappij dient derhalve de activiteiten van sociale netwerken te controleren en aan te vullen.

- Ouders verwachten dat scholen en ISP's een belangrijke rol spelen in de voorlichting – voor beide een waardevolle kans om zich die rol eigen te maken en reeds gestarte activiteiten te intensiveren.

- NGO's hebben al veel activiteiten ontplooid in brede kring – deze moeten in de nabije toekomst samengevoegd worden om de krachten te bundelen en grootschalige samenwerking te versterken, in het bijzonder met scholen.

- Samenwerking van ISP's met NGO's kan zorgen voor een groot bereik van de voorlichtingsmaterialen, zowel online als offline.

- Alle vormen van informatie moeten gericht zijn op de specifieke (leeftijds)groepen op het net. De opgroeiende "born digital" generatie heeft nauwelijks behoefte aan technische informatie, maar moeten wel de mogelijke negatieve gevolgen leren kennen van het op verkeerde wijze delen van persoonlijke gegevens en profielen online. Jonge kinderen hebben behoefte aan eenvoudig interactief advies; ouders moeten het online-gedrag van hun kinderen leren kennen en in staat zijn de symptomen van mogelijke blootstelling aan gevaren als grooming en in een vroeg stadium op te merken.

CASE 7: FILTEREN VAN AUTEURSRECHTELIJK BESCHERMDE CONTENT

***Probleem:** Onrechtmatig gekopieerde audio en video wordt massaal verspreid op het internet en de contentsector staat voor het probleem om digitale businessmodellen te vinden.*
***Risico:** Netwerkoperators worden gedwongen de toegang tot bepaalde content te beperken, wat mogelijk niet strookt met geldende wetgeving en de gebruikerservaring beperkt.*

Protocollen en platforms voor filesharing in combinatie met toenemende breedbandsnelheden maakt de strijd tegen illegaal kopiëren online tot een van de grootste huidige problemen houders van audiovisuele rechten en regelgevers.

De laatste tijd richten beleidslijnen voor het bestrijden van illegaal kopiëren zich steeds vaker op netwerkproviders en ISP's, die onder druk worden gezet om proactiever op te treden. Maatregelen die worden overwogen variëren van technologische oplossingen (bijvoorbeeld deep packet inspection en een aantal vormen van netwerk-gebaseerd filteren, het gebruik van digitale vingerafdrukken door hostingproviders of watermerken door contentproviders) tot niet-technologische maatregelen (zoals waarschuwen aan als overtreders geïdentificeerde klanten); zie casestudy 8.

Volgens EU-regels zijn netwerkoperators en ISP's, als "slechts een doorgeefluik", uitgezonderd van elke algemene verplichting om het verkeer over hun netwerken te monitoren. Ze hoeven alleen illegale content van servers te halen die ze zelf hosten nadat ze van het bestaan daarvan op de hoogte zijn gesteld. In het algemeen zijn ze tegen "actieve" internetfiltering ter bestrijding van inbreuk op copyright. De reden is dat de meeste technologische filters ofwel overblokkeren – met het gevaar wettelijk aansprakelijk gesteld te worden als legale content ten onrechte wordt geblokkeerd, of als legitiem gebruik, dat is vrijgesteld van auteursrechten en de vrijheid van informatie, wordt beperkt – ofwel onvoldoende blokkeren omdat copyrightschenders en nieuwe technologieën altijd wel een omweg vinden. Een vrijwillige of zelfs gereguleerde oplossing vinden is dan ook moeilijk. Het kan erg lastig zijn (of zelfs onmogelijk) voor een

** Tim Wu, hoogleraar in de Rechten, Columbia University*

netwerkoperator of ISP om een legaal aanbod te onderscheiden van een onrechtmatig aanbod als beide precies hetzelfde bestand gebruiken. Een "one size fits all" technologische aanpak die 100 procent doeltreffend is, bestaat niet.

Bovendien is er, in tegenstelling tot het filteren van kinderpornografie, geen overkoepelende politieke of publieke steun om – potentieel overblokkerende – maatregelen te tolereren die fundamentele internetvrijheid dreigen te beperken met als doel het beschermen van commerciele belangen (hoe legitiem ook) van een bepaalde belanghebbende.

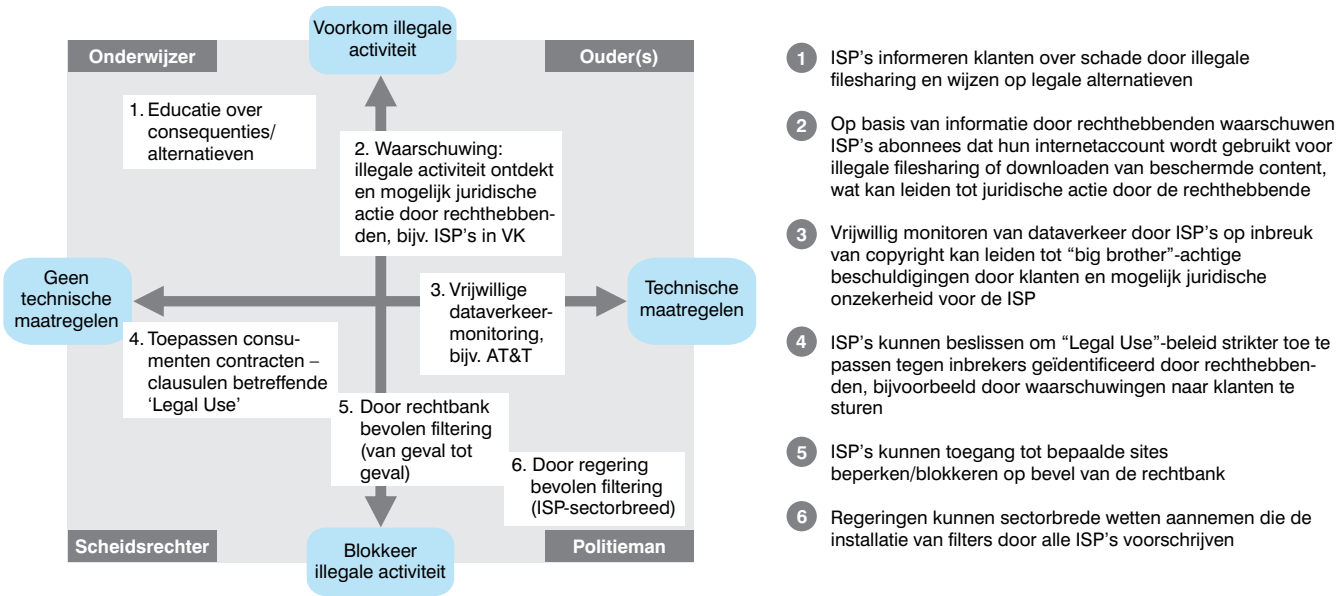
Toen AT&T in januari 2008 liet weten van plan te zijn om proactief alle verkeer te monitoren dat mogelijkerwijs de Amerikaanse wetten op intellectueel eigendom zou schenden, riep dat veel weerstand op bij de consumenten die "Big Brother"-praktijken voorzagen. Bovendien was er veel kritiek op het feit dat AT&T vrijwillig het gevaar zou lopen de immuniteit voor copyrightaansprakelijkheid te verliezen als zij actief de content die gebruik mocht maken van hun netwerken zou selecteren.

Verplicht filteren van content onder copyright wordt daarom alleen door gerechtelijke instanties opgelegd en van geval tot geval beoordeeld.

In een aangepaste versie van het generieke Digital Confidence Positioneringmodel kan filteren worden gezien als een vorm van reactie op illegale filesharing, die in twee dimensies bepaald kan worden (figuur 53). De verticale as differentieert wat er feitelijk gedaan wordt om illegale filesharing te bestrijden, van het voorkomen dat gebruikers zich bezighouden met illegale activiteiten tot het blokkeren van illegale activiteiten door filtering. De horizontale as reikt van niet-technische maatregelen gericht op het disciplineren van gebruikersgedrag tot technische maatregelen tegen filesharers en downloaders. Hier is filteren een rol van de Scheidsrechter als, bijvoorbeeld, een individuele ISP door een rechtbank wordt gelast de toegang tot een bepaalde P2P-site te blokkeren. Of het is een rol voor de Politieman als een complete ISP-sector door wetgeving wordt gelast om filters te installeren.

The Pirate Bay (TPB) is de laatste jaren een belangrijke bron van geschillen op dit gebied. Het is een van de bekendste en grootste BitTorrent-tracker- en -zoeksites. TPB heeft de naam veel door copyright beschermde (dus onrechtmatig gekopieerde) content te verspreiden, zoals films. Verschillende ISP's, bijvoorbeeld het Deense Tele2, werden onlangs gedwongen om TPB te blokkeren, zoals beschreven in figuur 54. Dit gedwongen blokkeren leidt tot twee grote problemen: technische toepasbaarheid en wettelijke goedkeuring. Wat betreft de techniek kan DNS-rerouting gebruikt worden om toegang tot TPB te beperken – maar gebruikers vinden altijd wel een manier om dit omzeilen. Of TPB voegt, zoals in het Deense voorbeeld, eenvoudigweg een andere domeinnaam toe die naar de site verwijst. Als alternatief kan TPB "geblackholed" worden. Dit is echter een zeer extreme maatregel aangezien alle diensten op hetzelfde IP-adres afgekapt zouden kunnen

Figuur 53: ***Digital Confidence positie t.a.v. filteren content met copyright***



worden (en ook dan zou het nog mogelijk zijn om deze blokkering te omzeilen).

In maart 2008 meldde de pers dat vier grote spelers op het gebied van muziek de Ierse ISP Eircom aanklaagden om internetgebruikers te laten stoppen met het onrechtmatig downloaden van muziek. Dit was het eerste geval in dat land waarbij een ISP aansprakelijk werd gesteld voor de handelingen van zijn klanten, in plaats van het individueel vervolgen van illegale downloaders. Dit volgde op een Belgische uitspraak in juni 2007, waarbij Scarlet, een van de toonaangevende ISP's in België, gelast werd binnen zes maanden een filteringoplossing te installeren. Deze beslissing leidde tot een heftige discussie of netwerkoperators al dan niet gedwongen kunnen worden om dataverkeer te blokkeren.

Ten slotte werd de strijd tegen illegaal kopiëren met gebruik van hightech filtering, als onderdeel van de netwerkmanagement middelen van de netwerkoperators, het middelpunt van de discussie over netneutraliteit in de Verenigde Staten. Rechtenhouders zoals MPAA en BC hebben opgeroepen tot een proactieve rol van de netwerkoperators door breedbandmanagement middelen in te zetten ter voorkoming van dataverkeer in onrechtmatig gekopieerde content. Zij stellen dat netneutraliteit de bescherming van intellectuele eigendom moet bevorderen en niet de ontwikkeling mag verhinderen van nieuwe filtertechnieken en identificatietechnologieën om schending van copyright op te sporen.

Aan de andere kant vergeleken consumentengroeperingen deze praktijk met censuur.

BELANGRIJKE LESSEN

Uit het bovenstaande kan een aantal belangrijke lessen getrokken worden:

- ISP's zijn in het algemeen erg terughoudend met proactief filteren van internetverkeer in de strijd tegen illegaal kopiëren. Een actieve rol betekent dat ISP's zich bemoeien met dataverkeer op hun netwerk en hun status ondermijnen van "doorgeefluik" dat hun immuniteit voor copyrightaansprakelijkheid verzekert en zich aldus blootstellen aan aanzienlijke juridische claims.

- Content filteren is zowel technisch als juridisch moeilijk te implementeren. Het leidt vrijwel zeker tot overblokkeren of juist onderblokkeren van autaursrechtschendende content en schending van "fair use" of citaatrecht. In tegenstelling tot het filteren van kinderpornografie bestaan er, voor zover wij weten, geen derde partijen die specifiek zwarte lijsten met illegale P2P-sites leveren, onderzoeken en actualiseren. Geautomatiseerde netwerkfilters gebaseerd op bijvoorbeeld digitale vingerafdrukken zijn wellicht in staat beschermde content te ontdekken, maar kunnen geen betrouwbaar oordeel geven of die content echt onrechtmatig gebruikt wordt of onder een uitzondering valt en legitiem gebruikt wordt. Daarnaast dient de fundamentele vraag te worden behandeld of het de

Figuur 54: ***The Pirate Bay – recente activiteiten***

The Pirate Bay

- 1 miljoen torrents
- 12 miljoen peers (gelijktijdig actieve verbindingen)
- 2,5 miljoen geregistreerde gebruikers

- Mei 2006: Politieoffensief tegen ThePirateBay (TPB)
  - Servers en andere apparatuur geconfisqueerd
  - Oprichters ondervraagd door de politie, maar niet aangeklaagd
  - Aangenomen wordt dat de MPAA de drijvende kracht achter het offensief was
  - In juni 2006 is TBP weer online
- Juli 2007: Zweden wil TPB op de zwarte lijst voor kinderpornografie zetten
  - Zou toegang vanuit Zweden geblokkeerd hebben
  - Beslissing herroepen – verwijten van kinderpornografie nooit bewezen
- September 2007: Geheime e-mails van MediaDefender tonen aan dat mediaconcerns hackers hebben ingehuurd voor DoS-aanvallen tegen TPB
- Januari 2008: TPB operators wordt "medeplichtigheid copyright-schending" verweten
- Februari 2008: Deens Tele2 krijgt opdracht klanten van TPB af te sluiten
  - IFPI beweert dat Tele2 copyright aantast door toegang tot TPB toe te staan
  - Hoger beroep – is in strijd met EU-wet volgens Tele2, aangezien kopiëren in routers expliciet is toegestaan in de EU Infosoc Richtlijn (artikel 5.1)
  - Dataverkeer vanuit Denemarken naar TPB toegenomen met 12% door publieke discussie
- Maart 2008: Zweedse ISP's gedaagd door IFPI om toegang tot TPB te blokkeren
  - Telia Sonera weigert aangezien het bespioneren van klanten niet rechtmatig zou zijn
  - Telia voelt zich niet verantwoordelijk voor acties van zijn klanten
- April 2008: TPB klaagt IFPI aan voor schadevergoeding door misgelopen Tele2 traffic

Bron: ThePirateBay, Wikipedia

verantwoordelijkheid is van de netwerkoperator om auteursrechtelijk beschermde content te beschermen. De kosten die dit met zich meebrengt worden dan vertaald in hogere tarieven voor zijn eigen aanbiedingen.

• In de paar gevallen dat netwerkoperators aankondigden van plan te zijn proactief internetverkeer te monitoren, kregen ze van de consumenten veel kritiek inzake klantprivacy vanwege de opdringerige aard van netwerk-gebaseerd filtertechnieken (bijvoorbeeld deep packet inspection en andere vormen). Bedrijven zetten hun concurrentiepositie op het spel tegenover operators die niet op deze manier filteren.

• In tegenstelling tot de discussie over kinderpornocontent kan het filteren van content voor de puur commerciële belangen van een bepaalde belanghebbende en daarmee het beperken van de fundamentele internetvrijheid, niet rekenen op brede politieke of publieke steun.

• Netwerk-gebaseerd filteren kreeg als kritiek dat het de principes van netneutraliteit geweld aandoet door onderscheid te maken tussen verschillende soorten internetverkeer en -diensten. Deze technieken zouden legitiem gebruik en legale meningsuiting in de weg staan, innovatie belemmeren en een gevaar vormen voor persoonlijke privacy. Bovendien zou het onderliggende probleem er niet mee aangepakt worden. Tegelijkertijd roepen copyrightshouders op tot het maken van een uitzondering op netneutraliteit om de bescherming van intellectuele eigendom te bevorderen en om filter- en identificatietechnologieën te verbeteren.

• Voorlichting van de consument speelt ook een belangrijke rol, maar heeft zijn beperkingen omdat de meeste gebruikers al weten wat ze doen.

CASE 8: "THREE STRIKES" TOEPASSEN

Probleem: ***In de poging om illegaal kopiëren te bestrijden wil de entertainmentindustrie de "three strikes"-regel introduceren: consumenten die tot drie keer toe auteursrechten schenden, worden afgesloten van het internet.***

Risico: ***Door het toepassen van de "three strikes"-regel kunnen honderdduizenden consumenten worden afgesloten van het internet, waardoor hun individuele rechten en de groei van de digitale economie ernstig kunnen worden beperkt.***

Naast technische oplossingen om copyrightschending tegen te gaan wordt er veel gesproken over niet-technische oplossingen om misbruik te verminderen op het niveau van de netwerkoperator en de ISP in de EU, de Verenigde Staten en Japan. De meest genoemde maatregel is de "three strikes and you're out"-regel, waarvoor copyrighthouders op de drie continenten actief campagne voeren: het idee is om consumenten die herhaaldelijk onrechtmatig downloaden van het internet te verbannen en een dergelijke regel in te zetten als afschrikmiddel zodat gebruikers überhaupt niet beginnen copyrightschendingen.

Vergeleken met het gericht blokkeren van diensten als The Pirate Bay, die voornamelijk (waarschijnlijk illegale) filesharing mogelijk maken of vergeleken met filteren van auteursrechtelijk beschermde content, bestaat het gevaar om het doel voorbij te schieten met het compleet verbannen van individuele gebruikers van het internet, alleen op grond van het schenden van copyright. Het is zeer de vraag of de commerciële belangen van één specifieke bedrijfstak voldoende reden zijn om individuen uit te sluiten van de digitale wereld. Daarnaast is het de vraag of netwerkoperators wel het recht hebben om deze rol te spelen. Iemand het gebruik van internet ontzeggen is een zware straf en moet misschien alleen worden uitgevoerd nadat juridische procedures uitgeput zijn. Als netwerkoperators, particuliere partijen, beslissen om iemand te verbannen op grond van bewijs van belanghebbenden, treden ze op als rechter en jury. De CEO van Carphone Warehouse, Charles Dunstone: "Onze opstelling is duidelijk. Wij geven gebruikers toegang tot het internet. Wij controleren het internet niet en wat onze gebruikers op het internet doen controleren wij ook niet. Ik zie geen omstandigheden waaronder wij, op grond van beschuldigingen door derden, vrijwillig de account van een van onze klanten zouden afsluiten"

De "three strikes, you're out"-regel maakt deel uit van het scala aan aantal mogelijke oplossingen om verboden filesharing tegen te gaan, zoals getoond wordt in figuur 55 en beschreven in case 7. De Onderwijzerreactie op de ontdekking van verboden filesharing zou bestaan uit het op de hoogte brengen van de gebruiker van de schade die wordt aangericht door illegale filesharing of downloaden van files onder auteursrecht en het aandragen van alternatieven voor dit illegale gedrag. Een niveau zwaarder is de Ouderaanpak. Hierbij waarschuwt de netwerkoperator proactief individuele gebruikers, op basis van informatie van copyrighthouderen, dat hun intellectuele eigendom door een computer die gekoppeld is aan het internetaccount van de betreffende persoon

wordt misbruikt. Er wordt uitgelegd dat dit gedrag bestaande copyrights schendt en kan leiden tot gerechtelijke stappen door de eigenaar van de rechten. Op basis van deze aanpak kan de netwerkprovider suggesties doen voor beveiligingssoftware om onrechtmatig downloaden op het account van de betrokkene tegen te gaan. Op deze manier minimaliseren netwerkoperators aansprakelijkheid en helpen hun klanten te begrijpen dat zij niet 100 procent anoniem zijn op het internet.

*Guy Bono, lid van het Europees Parlement: "Over dit onderwerp kan ik zeggen dat ik het oneens ben met sommige lidstaten die strenge maatregelen nemen, opgelegd door een industrie die er niet in is geslaagd haar werkwijze aan te passen aan de eisen van de informatiemaatschappij. Het afsluiten van het internet is een buitenproportionele maatregel ten opzichte van het beoogde doel. Het is een sanctie die grote gevolgen kan hebben in een samenleving waarin toegang tot het internet absoluut noodzakelijk is voor deelname aan het sociale leven." **

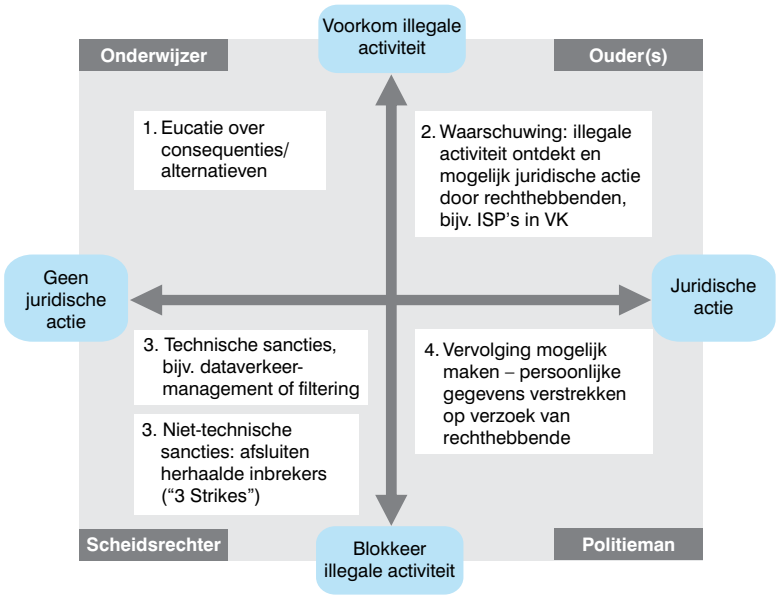
Deze aanpak wordt momenteel geïmplementeerd door zes toonaangevende ISP's in Groot-Brittannië. Virgin Media en British Phonographic Industry (BPI) hebben middels een test het effect van waarschuwingsbrieven bekeken. In juli 2008 heeft dit geleid tot een voorstel voor co-regulering op basis van een Memorandum of Understanding, gefaciliteerd door de regelgevende instantie OFCOM. Dit memorandum biedt een basis om actie te kunnen ondernemen tegen het onwettig gebruik van P2P-technologie. Het is ondertekend door de BPI en MPAA als vertegenwoordigers van de copyrighthouders, door Virgin Media, BSkyB, BT, Orange, Tiscali en Carphone Warehouse als ISP's en door drie betrokken Ministeries. De betrokken ISP's zijn overeengekomen om bij wijze van proef gedurende drie maanden eerst 1.000 van hun klanten aan te schrijven die door de eigenaren van auteursrechten zijn geïdentificeerd. Als aanvulling hierop wordt een gedragsprotocol opgesteld – dat goedkeuring van de OFCOM vereist – waarin opgenomen: vereisten voor bewijs; acties tegen vermoedelijke misbruikers en bij herhaald en crimineel misbruik; schadeloosstelling voortkomende uit onterechte beschuldigingen van onrechtmatige filesharing en klachtenprocedures voor consumenten. Tot nog toe dreigen de Britse ISP's hun klanten nog niet met afsluiting. Bij hun waarschuwingsbrieven wordt echter een schriftelijke waarschuwing van de BPI gevoegd, waarin gedreigd wordt met afsluiting en rechtszaken tegen degenen die toch doorgaan met onrechtmatig downloaden. Oplossingen voor herhaaldelijke overtreders die ongevoelig zijn voor dergelijke brieven wordt nog besproken. Overwogen worden onder meer technische middelen, zoals dataverkeermanagement of filteren en het herkenbaar maken van files om identificatie te vergemakkelijken.

De derde mogelijke aanpak, filteren van specifieke files of filesharing-sites, werd in detail besproken bij de vorige case.

De meest interventionistische aanpak – afsluiten – is momenteel onderwerp van discussie en in sommige landen al geïntroduceerd als de "three strikes and you're out"-aanpak.

** http://www.cablefo-rum.co.uk/article/397/european-parliament-rejects-3-strikes-rule-is-vm-listening*

Figuur 55: *Digital Confidence positie t.a.v. "Three Strikes" regel*



1. ISP's informeren klanten over schade door illegale filesharing en wijzen op legale alternatieven
2. Op basis van informatie door rechthebbenden waarschuw ISP's abonnees dat hun internetaccount wordt gebruikt vo illegale filesharing, wat kan leiden tot juridische actie door de rechthebbende
3. ISP is verplicht (door co-regulering of wetgeving) contractu ele "Legal Use" bepalingen toe te passen tegen copyright- schenders (geïdentificeerd door rechthebbende) en direct actie te ondernemen:
   - Technische maatregelen, zoals filters, dataverkeer-management
   - Niet-technische maatregelen: (tijdelijk) internettoegang afsluiten – "Three Strikes" is een combinatie van waarschuwingsproces en actieve interventie
4. ISP bij wet verplicht persoonlijke gegevens te verstrekken van het betrokken IP-adres op verzoek rechthebbende – zonder bevel van de rechtbank tot civiele actie – rechtsgrond dient gecontroleerd te worden in data bescherming wetgeving

Noot: Voor een gedetailleerde discussie over filteren van content met copyright zie case 7

Concreet dient het volgende te gebeuren (naar het voorbeeld van Frankrijk, waar het bekendstaat als het "Accord Olivennes", genoemd naar Denis Olivennes, CEO van de grote Franse mediaonderneming FNAC en voorzitter van het comité dat de overeenkomst heeft opgesteld en aangeboden aan president Sarkozy): ISP's moeten waarschuwingen verzenden en sancties opleggen zoals voorgeschreven door de nieuw opgerichte autoriteit tegen illegaal kopiëren HADOPI, die overtredingen gemeld krijgt door de copyrighthouders en op grond hiervan instructies stuurt naar de ISP's. ISP's moeten twee waarschuwingen sturen naar verdachten van overtredingen. De eerste per e-mail. In geval van het uitblijven van een reactie en blijvende overtreding, volgt een tweede waarschuwing per aangetekende brief met ontvangstbewijs. Als er dan nog geen reactie komt en de illegale activiteit blijft doorgaan, wordt de account gedurende vijftien dagen afgesloten. Als er dan nog steeds geen reactie volgt en het misbruik na het opnieuw aansluiten blijft doorgaan, kan de account maximaal een jaar worden afgesloten.

Algemeen gesproken bestaat er nog grote onduidelijkheid over hoe de "three strikes"-regel kan worden geïmplementeerd. Er zijn bijvoorbeeld verschillen van mening over de duur van afsluitingen; hoe het proces te monitoren (in Frankrijk wordt gesproken over een landelijk register van overtreders); variërende discussies over de verantwoordelijkheid in verschillende landen (vooral of netwerkoperators en ISP's alle overtredingen moeten opsporen of alleen reageren op overtredingen gemeld door copyrighthouders); aansprakelijkheid (ingeval van onterechte beschuldiging van overtreders); en ten slotte wie dit alles moet betalen.

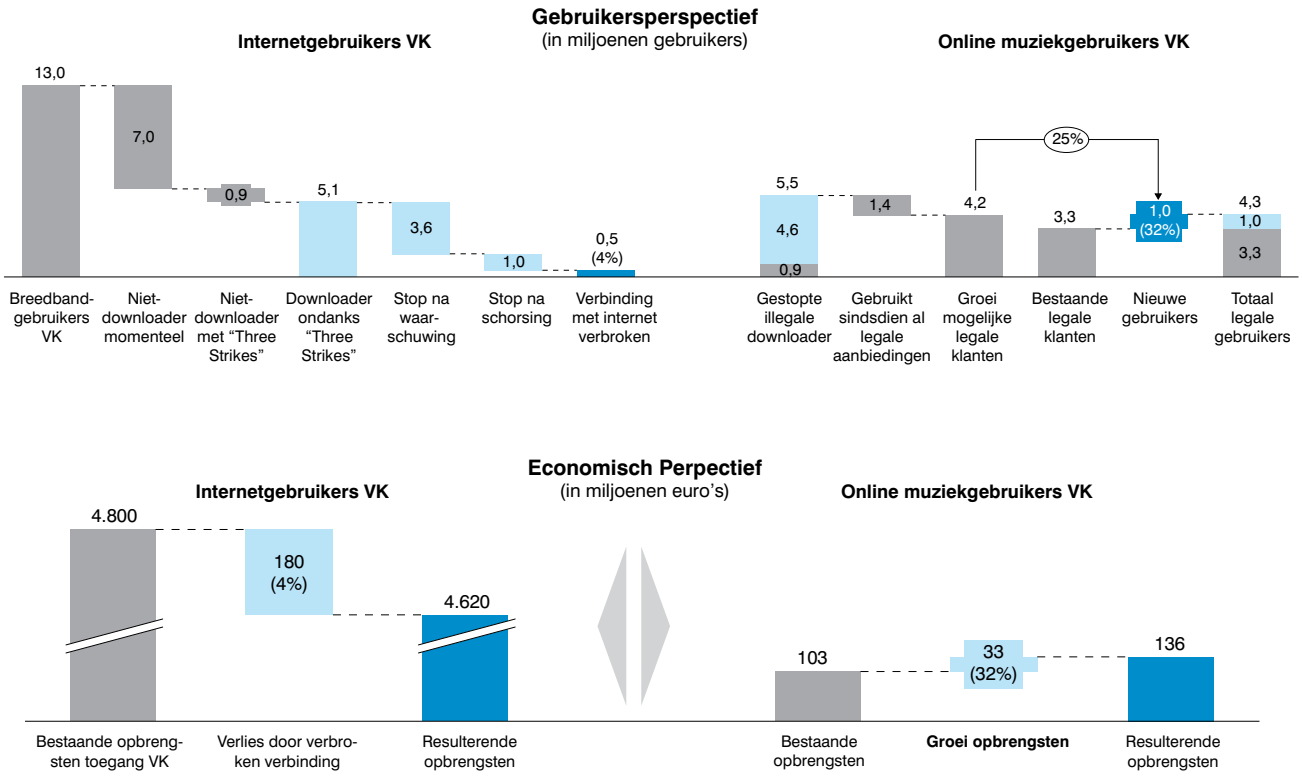
Landen denken verschillend over de "three strikes"-regel. Frankrijk lijkt het verst gevorderd in het formuleren van de aanpak in de vorm van een wetsvoorstel dat in de herfst van 2008 wordt besproken in het parlement.

In Frankrijk is de medewerking van de belangrijkste ISP's verkregen via een "deal" waarbinnen onder meer geregeld is dat het legaal downloaden van muziek DRM-vrij wordt aangeboden. Aanvankelijk leek Groot-Brittannië de Franse aanpak te

*"De zes grootste internetproviders in Groot-Brittannië hebben een door de regering gesteund convenant ondertekend om af te rekenen met het illegale muziek-filesharing. De zes providers – BT, Virgin Media, Orange, Tiscali, Sky en Carphone Warehouse – zullen maatregelen implementeren tegen degenen die betrapt worden op filesharing. De ISP's zijn niet bereid de door de BPI geprefereerde "Three strikes en je ligt eruit"-aanpak, waarbij gebruikers worden afgesloten van hun breedbandverbindingen, toe te passen." **

** BBC News, 24 juli 2008*

Figuur 56: *"Three Strikes" implementeren in de VK – indicatieve sensitiviteitsanalyse*



Bron: Nieuwsrapporten, Europese commissie

volgen en actief van plan te zijn om het te implementeren indien ISP's en rechtenhouders niet tot een akkoord zouden komen. Maar in de hierboven besproken overeenkomst tussen netwerkoperators, ISP's en copyrighthouders is het afsluiten van herhaaldelijke overtreders niet meer opgenomen als te overwegen remedie. De aanpak in Groot-Brittannië is gekoppeld aan de belofte door de ondertekenaars partijen om commercieel aantrekkelijke legale aanbiedingen (lidmaatschap, on-demand, sharing) te doen als alternatief voor illegale filesharing.

In Japan zijn de vier belangrijkste ISP's overeengekomen om de "three strikes"-regel te implementeren als reactie op druk vanuit de overheid en de bedrijfstak.

In april 2008 heeft het Europese Parlement de "three strikes"-aanpak afgewezen toen werd gestemd over een rapport over het bevorderen van Europese culturele industrieën.

Als laatste wordt "three strikes" genoemd als een van de mogelijke technische verplichtingen voor ISP's die besproken worden in de context van de Anti-Counterfeiting Trade Agreement (ACTA) van de G8, die dit voor eind 2008 willen afronden. De ACTA betreft voor een groot deel het actualiseren van juridische kaders zodat die P2P en ontwikkelingen op het internet in acht nemen. Hoewel de onderhandelingen plaatsvinden achter gesloten deuren is uitgelekt dat "three strikes" en verplichte filtering door ISP's op de agenda staan.

Een aspect dat in de publieke discussie over "three strikes" vaak buiten beeld blijft is de mogelijke schade voor de digitale economie als grote aantallen consumenten worden afgesloten van het internet. De gevolgen van "three strikes" moeten holistischer worden bezien. Een gevoeligheidsberekening voor bijvoorbeeld Groot-Brittannië schat dat de "three strikes"-methode kan resulteren in het afsluiten van 500.000 gebruikers en een verlies aan inkomsten van £180 miljoen bij netwerkoperators (figuur 56). De inkomsten van de muziekindustrie stijgen daarentegen slechts met ongeveer £33 miljoen. Dit totale inkomstenverlies van £150 miljoen is waarschijnlijk maar een klein deel van het negatieve effect voor andere belanghebbenden, bijvoorbeeld door de afname in het totale e-commerce-volume.

Naast het feit dat burgers worden uitgesloten van de digitale wereld, maakt de potentiële economische schade in de hele waardeketen van de digitale economie "three strikes" een lastig concept bij het vinden van een proportionele remedie tegen illegaal kopiëren.

BELANGRIJKE LESSEN

Uit het bovenstaande kunnen drie belangrijke lessen getrokken worden:

- Met het "three strikes"-principe wordt bij het bestrijden van copyrightschending in toenemende mate ingegrepen in het internetverkeer, met een aanzienlijk risico op "doorschieten" als de implicaties niet evenwichtig worden afgewogen.

- Het is twijfelachtig of de commerciële belangen van een bepaalde bedrijfstak voldoende reden zijn om mensen uit te sluiten van de digitale wereld – zeker gezien de kosten die implementatie en uitvoer met zich meebrengen voor andere belanghebbenden binnen de digitale economie.

- Het debat omtrent "three strikes" spitst zich toe op de vraag of de strategie zelf wel geschikt is – noodzakelijke voorwaarden, vooral de problemen rond het correct detecteren van copyrightschendingen en bredere implicaties zijn onvoldoende behandeld.

- Overheden en netwerkoperators in de verschillende landen hebben uiteenlopende maatregelen genomen. Het Europese Parlement roept in zijn resolutie over "Cultural Industries in Europe" (april 2008) netwerkoperators en contenteigenaren op tot samenwerking en spreekt zich specifiek uit tegen maatregelen die consumenten zonder winstbejag criminaliseren als zijnde een onjuiste manier om illegaal kopiëren te bestrijden. Duidelijk verwijzend naar Franse aanpak roept het parlement op maatregelen te vermijden die in strijd zijn "met burgerlijke vrijheden en mensenrechten en met de principes van proportionaliteit, doeltreffendheid en ontmoediging, zoals het onderbreken van internettoegang."

2. AGENDA VAN DE REGELGEVERS

Wat betreft Digital Confidence kunnen de regulerende activiteiten van overheden op Europees en nationaal niveau in zes groepen worden ondergebracht:

- Activiteiten in verband met het herzien van de bestaande wetgeving voor providers rond van elektronische communicatie-infrastructuren en communicatiediensten.

- Activiteiten gerelateerd aan de herinterpretatie van juridische principes zoals de EU-richtlijn Gegevensbescherming.

• Activiteiten gericht op het verbeteren van samenwerking tussen de diverse belanghebbenden in de industrie.

• Gezamenlijk gesponsorde initiatieven.

• Wetgevende activiteiten op nationaal niveau.

• Activiteiten gericht op internationale coördinatie.

2.1 AANPASSING VAN DE WETGEVING EN TE VOLGEN STRATEGIE

In november 2207 heeft de Europese Commissie een herziening voorgesteld van de Europese regelgeving – een Review of the European Regulatory Framework – voor providers van elektronische communicatie-infrastructuren en -diensten. De commissie denkt dat de voorstellen tot wetten worden vóór eind 2009.

Tegen de achtergrond van de toenemende dreiging van spam, spyware, virussen en phishing, wil de Review de bestaande netwerken versterken en oudere wetgeving die bepaalde activiteiten criminaliseert aanvullen. Ten aanzien van Digital Confidence zijn de doelstellingen van de Review voornamelijk gericht op:

• Vergroten van consumentenbewustzijn en hulpmiddelen, vooral ten aanzien van inbreuken op netwerkbeveiliging en e-privacy. De commissie introduceert bijvoorbeeld het concept van het verplicht rapporteren van inbreuken op de beveiliging door netwerkoperators en ISP's.

• Verbeteren van de gebruikerservaring door het stimuleren van ongehinderde toegang tot digitale en onlinediensten door de nationale regulerende autoriteiten de mogelijkheid te geven worden minimale eisen voor de Quality of Service op te leggen.

Met betrekking tot netwerkbeveiliging en privacy van de gebruiker wordt in de Review voorgesteld dat:

• Consumenten door de ISP's worden ingelicht als hun persoonlijke gegevens in gevaar komen door fouten in de beveiliging.

• Operators en regelgevers meer verantwoordelijkheid krijgen inzake de beveiliging en integriteit van electronische communicatienetwerken en -diensten.

• Handhavende - en implementatiemogelijkheden voor de betrokken autoriteiten worden vergroot, met name in het gevecht tegen spam.

• De EU-regels over gegevensverzameling en identificatieapparatuur met gebruik van elektronische communicatienetwerken worden verduidelijkt.

Ten aanzien van tot het veiligstellen van consumententoegang tot hoogwaardige digitale en online-diensten in de toekomst stelt de review dat:

• De nationale regelgevende autoriteiten minimumeisen mogen stellen aan de QoS van netwerkproviders voor elektronische communicatie op basis van normen ontwikkeld op EU-niveau.

Het doel is te voorkomen dat diensten degraderen en de netwerksnelheid zo ver afneemt dat de connectiviteit ernstig gevaar loopt. Volgens informatie van Viviane Reding, Europees Commissaris voor Informatiemaatschappij, is er nog steeds ruimte om dataverkeer over de netwerken te managen en te shapen teneinde de gebruikerservaring te optimaliseren, op voorwaarde dat dit op transparante, proportionele en niet-discriminerende wijze gebeurt.

De Review doet ook uitspraken over de onafhankelijkheid van het European Network & Information Security Agency (ENISA), gevestigd op Kreta. In 2004 opgericht met het oog op de steeds toenemende afhankelijkheid van ICT in essentiële zakelijke processen, probeert ENISA onder andere zakelijke continuïteit te stimuleren door het vaststellen van best practices en het ontwikkelen van risicobeperkende normen voor de behandeling van ontwrichtende incidenten in de verschillende infrastructuren zoals kwaadwillige IT-aanvallen of het verlies van essentiële gegevens. Tot op heden heeft ENISA een aantal aanbevelingen gedaan, onder meer over beveiligingskwesties voor online sociale netwerken, botnets en reputation based-systemen (bekende spam-verzenders). In verband met zorgen over de effectiviteit van ENISA als leverancier van actuele operationele ondersteuning aan bedrijven, stelde de commissie een fusie voor tussen ENISA en een nieuw op te richten Europese regelgevende instantie. Aangezien dit voorstel van een nieuwe Europese regelgevende instantie zeer controversieel bleek, is onduidelijk of de ENISA gaat fuseren of onafhankelijk blijft. Desondanks heeft de EU besloten het mandaat van de ENISA te verlengen tot 2011, wanneer de nieuwe Europese regelgevende instantie – indien opgericht – het overneemt.

2.2 OPNIEUW INTERPRETEREN VAN BESTAANDE WETGEVING

Het herinterpreteren van wetgeving gebeurt vooral in het veld van databescherming en privacy. De huidige ontwikkelingen in Web 2.0-services en de ermee samenhangende business-modellen, bijvoorbeeld behavioural en viral marketing, zoektechnologie en sociale netwerken, vormen een probleem voor geldende principes voor gegevensbescherming zoals transparantie, informed consent (recht op toestemming), purpose limitation (doelbinding) en het recht op rectificatie zoals vastgelegd in de EU-richtlijn Gegevensbescherming (1995).

VOORBEELDEN VAN DE VOORTGAANDE DISCUSSIE OVER REGULERING

Japan: "Richtlijnen voor Dataverkeer Shaping", mei 2008

In Japan, vaak genoemd als een van de meest geavanceerde markten in beschikbare snelheden en de inzet van NGN, hebben vier instellingen uit de telecomindustrie (Japan Internet Providers Association, Telecommunications Carriers Association, Telecom Service Association, Japan Cable en Telecommunications Association) in mei 2008 richtlijnen voor dataverkeer-shaping aanvaard. Volgens een onderzoek van het Japans Ministerie voor Communicatie in november 2007 maakte 40 procent van de Japanse ISP's gebruik van snelheidsregulering.

De richtlijnen proberen, naar aanleiding van de grote toename in verkeer door P2P-filesharing, snelheden voor grootgebruikers te beperken. Het Japanse ministerie van Binnenlandse Zaken en Communicatie observeert de richtlijnen die de minimale normen voor dataverkeer-shaping vastleggen, waarop elke ISP zijn eigen beleid zal baseren en implementeren. De richtlijnen zijn vrijwillig – de principes die erin geschetst worden, moeten leiden tot een "veilige haven" van gedrag dat als wettig zal worden beschouwd.

De richtlijnen stellen dat ISP's in principe toenames in de hoeveelheid communicatie moeten opvangen door hun faciliteiten te verbeteren. Het beperken van de snelheid mag alleen in uitzonderlijke gevallen worden overwogen. Zo kunnen providers de communicatiesnelheid beperken voor grootverbruikers van speciale software zoals P2P-programma's, of voor degenen die heel veel data willen uploaden boven een bepaalde grens, als hun handelingen een groot deel van het netwerk in beslag nemen en aldus de communicatie van andere gebruikers hinderen. In dergelijke gevallen zijn ISP's verplicht de informatie over deze beperkende maatregelen bekend te makan een de gebruikers.

De minimale basisnormen houden verband met 1) het bereik van de noodzakelijke informatie voor de contractovereenkomst; 2) fundamentele eisen voor dataverkeer-shaping; 3) relevante juridische interpretatie.

De richtlijn onderzoekt de mogelijkheden om de bandbreedte te beperken voor specifieke toepassingen of gebruikers die het netwerk buitenproportioneel beïnvloeden ten nadele van algemene gebruikers.

Erkend wordt dat er privacybelangen meespelen in het geval van DPI bij packet-shaping (bijvoorbeeld het briefgeheim) en verklaart de mogelijkheid van bepaalde "gebruikerstoestemming"-vereisten, maar presenteert de juridische grond voor een uitzondering op de privacy- en toestemmingeisen waar er een "wettelijk gerechtvaardigde basis is voor "packetshaping".

Er worden voorbeelden gegeven van gevallen waarin dataverkeer-shaping wettelijk te rechtvaardigen is – om het gebruik van een specifieke toepassing of van een specifieke gebruiker te beperken – gericht op 1) gerechtvaardigd doel; 2) noodzaak van actie; 3) rechtsgeldige middelen.

Deze voorbeelden zijn niet uitputtend; er wordt onderkend dat er nieuwe handelswijzen ontwikkeld zullen worden, en dientengevolge worden de eisen op hoog niveau gehouden en blijven gericht op het veiligstellen van stabiele netwerken.

De richtlijnen adviseren een wijdverbreide kennisgeving van de inzet van packet-shaping (in tegenstelling tot de noodzaak van instemming) en bevelen aan dat deze kennisgeving duidelijk is voor eindgebruikers, niet-eindgebruikers en andere ISP's (vooral downstream-ISP's).

Groot-Brittannië: Ofcom's "Vrijwillige gedragscode: breedbandsnelheden", mei 2008

In Groot-Brittannië adverteren breedbandinternetproviders met de hoogste snelheden die hun netwerken maximaal aankunnen. Afhankelijk van technologie, infrastructuur en omgeving kan deze geadverteerde maximale bandbreedte niet worden bereikt door specifieke klanten.

De nieuwe code vereist dat netwerkproviders een accurate schatting maken van de maximaal bereikbare snelheid over hun verbinding. Bovendien eist de code dat gegevens over de toepassing van dataverkeer-shaping en relevante regels roden gepubliceerd (bijvoorbeeld de betreffende protocollen en toepassingen, "fair use"-limiet).

Ofcom gaat breedbandsnelheden verder onderzoeken en erkent reeds dat snelheden aanzienlijk kunnen afwijken van geclaimde maximale snelheden. In de toekomst kan de publicatie van de gemiddelde snelheid ook onderdeel van de code worden

De artikel 29 werkgroep Gegevensbescherming is voortdurend bezig de toepassing van de bestaande wetgeving uit de EU-richtlijn Gegevensbescherming op nieuwe technologieën te onderzoeken. Recentelijk heeft de Groep een nieuw Advies aangenomen ten aanzien van kwesties inzake gegevensbescherming in verband met zoekmachines. Een belangrijke conclusie in dit Advies is dat de Richtlijn Gegevensbescherming van toepassing is op het verwerken van persoonlijke data door zoekmachines. Providers van zoekmachines moeten persoonlijke data verwijderen of onomkeerbaar anoniem maken zodra ze niet meer nodig zijn voor het legitieme en gespecificeerde doel waarvoor ze verzameld zijn en in staat zijn het behoud ervan en de levensduur van ingezette "cookies" te allen tijde te rechtvaardigen. Voor elk het leggen van kruisverbanden tussen gebruikersdata en het verrijken van gebruikersprofielen dient de toestemming van de gebruiker te worden verkregen. Opt-outs van de website-editor dienen altijd door de zoekmachine te worden gerespecteerd en verzoeken van gebruikers om caches te actualiseren/vernieuwen moeten direct worden ingewilligd. Controverse ontstond vooral over het feit dat de Groep IP-adressen als persoonlijke data interpreteerde.

De toekomstige prioriteiten van de Groep omvatten onderzoek betreffende het zekerstellen van gegevensbescherming in relatie tot nieuwe technologieën, onder meer gericht op online sociale netwerken (met name voor kinderen en tieners), gedragprofilering, datamining (on- en offline) en digital broadcasting.

2.3 SAMENWERKING MET BELANGHEBBENDEN FACILITEREN

Gezien de snelle veranderingen in de markt, businessmodellen en technologieën worden snelle en doelmatige oplossingen door samenwerkende belanghebbenden steeds meer verkozen boven nieuwe wetgeving. Op het gebied van de bestrijding van illegaal kopiëren van content onder auteursrecht wil de commissie komen tot het oprichten van een discussie- en samenwerkingsplatform voor belanghebbenden, het zogenaamde "Platform Onine-Inhoud". Consumenten krijgen een belangrijke stem in dit platform.

In navolging van de communicatie over "Creatieve Online-Inhoud in de Interne Markt" uit 2008 wil de commissie komen tot een gedragscode voor toegang-/serviceproviders, rechthebbenden en consumenten om te zorgen voor een adequate bescherming van auteursrechten en hechte samenwerking in de strijd tegen illegaal kopiëren en ongeoorloofde filesharing

2.4 GESPONSORDE INITIATIEVEN TER ONDERSTEUNING VAN DIGITAL CONFIDENCE

Begin 2008 heeft de commissie een voorstel gedaan voor een nieuw Safer Internet-programma om de veiligheid van kinderen online te verbeteren. Het nieuwe programma bouwt verder op het Safer Internet-programma opgestart in 2005 en zal ook de recente communicatiediensten uit het Web 2.0-tijdperk, zoals sociaal netwerken, omvatten. Het voorgestelde nieuwe programma zal programma's medefinancieren die:

- Nationale contactpunten bieden waar illegale en schadelijke online-content gemeld kan worden, met name betreffende kindermisbruik en grooming.

- Initiatieven aanmoedigen om hierin tot zelfregulering te komen en de betrokkenheid van kinderen in het realiseren van een veiliger online-omgeving stimuleren.

- Bewustwording van kinderen, ouders en onderwijzers stimuleren en contactpunten ondersteunen waar ze advies kunnen krijgen over veiligheid online.

• Een kennisbank oprichten over het gebruik van nieuwe technologieën en de bijbehorende gevaren door het samenbrengen van onderzoekers op het gebied van veiligheid online voor kinderen op Europees niveau.

Aanbevelingen door kinderen zelf tijdens een Europees jongerenforum op Safer Internet Day in februari 2008 maken deel uit van de voorstellen. Het voorgestelde nieuwe Safer Internet-programma (2009-2013) wordt naar verwachting in 2009 aangenomen. De medefinanciering van projecten begint in 2010.

Voorbeelden van door het 2005 Safer Internet-programma gefinancierde projecten zijn "Insafe" (burgers de mogelijkheid bieden van positief en veilig internetgebruik door best practices, informatie en technieken te delen in samenwerking met de industrie, scholen en families) en "INHOPE" (wereldwijde ondersteuning van internethotlines waar illegale content zoals kinderpornografie gemeld kan worden; zie ook de bespreking van het beschermen van minderjarigen in hoofdstuk IV-1).

2.5 NATIONALE BENADERINGSWIJZEN

Er bestaan belangrijke verschillen in de manier waarop de verschillende individuele landen omgaan met de bedreigingen van Digital Confidence. Ze zijn vooral zichtbaar in het gevecht tegen illegaal kopiëren. De Franse aanpak, het Accord Olivennes – waarmee onrechtmatige downloaders op basis van het "three strikes"-principe tijdelijk de toegang tot het internet wordt ontzegd – vertegenwoordigt de ene kant van de schaal waarop de nationale benaderingen kunnen worden weergegeven. De Nederlandse aanpak – gebaseerd op de "notice and takedown"-aanpak waarbij zelfregulatie door ISP's vooropstaat – is een voorbeeld van de andere kant van het spectrum. De Franse aanpak waarbij onrechtmatige downloaders worden gestraft is het tegenovergestelde van de aanpak in de Verenigde Staten, waar uploaders in plaats van downloaders het doel zijn van "notice and takedown"-procedures. Ongeautoriseerd uploaden van materiaal onder copyright is onrechtmatig in Frankrijk, maar het Accord Olivennes biedt geen juridische ondersteuning om met technische maatregelen uploaders te pakken. Volgens het Accord Olivennes dienen ISP's content te identificeren (met vingerafdruk en/of watermerken) en de autoriteiten te verwittigen zodat actie tegen gebruikers wordt genomen.

Eerder, in januari 2008 besloot het Europese Hof van Justitie in een zaak aangaande de handhaving van intellectuele eigendomsrechten dat de Europese richtlijnen betreffende gegevensbescherming en e-privacy niet vereisen dat aan netwerkoperators verplichtingen worden opgelegd om in civiele zaken persoonlijke data van onrechtmatige downloaders openbaar te maken zodat rechthebbenden tot vervolging over kunnen gaan. In dit geval had de Spaanse vereniging van rechthebbenden (Promusicae) het Spaanse Hof gevraagd Telefonica te verplichten de identiteit en de huisadressen vrij te geven van klanten die gebruik hadden gemaakt van de Kazaa P2P-dienst voor onrechtmatige muziek-filesharing. Net als in de resolutie van het Europees Parlement werd de afweging van bescherming van fundamentele rechten tegenover de bescherming van (intellectueel) eigendom besloten in het voordeel van het beschermen van fundamentele burgerrechten, in dit geval het recht op privacy.

Frankrijk heeft, in haar rol als voorzitter van de EU gedurende de tweede helft van 2008, aangekondigd dat haar doelstellingen inzake het beleid omtrent intellectueel eigendom niet het exact nastreven van een Accord Olivennes op Europees niveau inhoudt. Het Franse presidentschap stelt zich in plaats daarvan ten doel om alle belanghebbenden om de tafel te krijgen om te onderhandelen.

Ten slotte behoort "three strikes" tot de voorstellen die actief worden besproken op G8-niveau. De Anti-Counterfeiting Trade

Militaire botnets in de informatieoorlog *

In mei 2008 stelde kolonel Charles W. Williamson III voor dat de Amerikaanse luchtmacht haar eigen zombie netwerk moet bouwen, zodat het DoS-aanvallen kan uitvoeren op buitenlandse vijanden. Hij raadt aan dat de luchtmacht bots installeert op zowel ongeclassificeerde computers als op de computers van de burgerlijke overheid.

Aanvankelijk stelden andere officieren van de US Navy voor om zelfs bots te installeren op bestaande informatiebeveiligingssystemen en om van computers die niet meer gebruikt worden een "botleger" te maken.

Burgercommentators van het bekende tijdschrift Wired noemden dit "het krankzinnigste idee sinds de homobom". Aan de andere kant kan de effectiviteit van grote DoS-aanvallen niet worden ontkend – zoals recent in Rusland waar hackers met een DoS-aanval het grootste deel van de Russische nucleaire energie-websites uit de lucht haalden.

** Bron: Wired, Darkreading*

Agreement (ACTA), die de G8 eind 2008 wil aannemen, kan "three strikes" omvatten en verplicht filteren door ISP's in een poging om de nieuwste P2P- en internetuitdagingen aan te pakken in de strijd tegen illegaal kopiëren en bijpassende straffen te kunnen opleggen.

2.6 INTERNATIONALE COÖRDINATIE

Na de DoS-aanvallen in Estland (vgl. case 6) werd tijdens de NAVO-bijeenkomst te Boekarest begin april 2008, besloten tot een algemene strategie voor "cyber defence" en de oprichting van een nieuwe instelling met als primaire taak de "politieke en technische" -reacties vanuit de NAVO op cyberaanvallen te coördineren.

Naast een nieuwe instelling is het voor een werkelijk gemeenschappelijk Europese aanpak van cyberverdediging noodzakelijk dat iedere lidstaat een eigen nationale structuur opbouwt ter voorkoming van en verdediging tegen cyberaanvallen, zoals in de Verenigde Staten het Computer Emergency Readiness Team (US-CERT), een partnership tussen het Department of Homeland Security en publieke en private sectoren. Het US-CERT werd in 2003 opgericht om de nationale internetinfrastructuur te beschermen en coördineert de beveiliging tegen en reactie op cyberaanvallen in het hele land. Zulke structuren bestaan op dit moment slechts in enkele Europese landen.

Europees Commissaris voor Informatiemaatschappij en Viviane Reding heeft aangekondigd dat de commissie begin 2009 een Mededeling zal doen over de bescherming van essentiële infrastructuur voor telecommunicatie. Deze zal gericht zijn op het verbeteren van de voorbereidingen en het reactievermogen op Europees niveau in geval van cyberaanvallen. De commissaris onderstreepte het belang van technische ontwikkelingen, zonder voorbij te gaan aan de noodzaak van meer voorlichting over de voordelen en de gevaren van de informatiemaatschappij. Deze aanpak lijkt veel steun te vinden in de bedrijfstak.

2.7 CONCLUSIE

De wettelijke basis voor het verminderen van de problemen met Digital Confidence lijkt grotendeels aanwezig, al bestaat de noodzaak tot herinterpretatie van bestaande regelgeving om de realiteit van nieuwe technologieën, marketing en gebruik in acht te nemen. De grensoverschrijdende aard van bedreigingen van Digital Confidence legt bijzondere nadruk op internationale (juridische) samenwerking, het vergroten van het bewustzijn van de dringende noodzaak tot handelen en, voor overheden en wetshandhavende instanties, het toewijzen van passende middelen voor het vaststellen van doeltreffende mitigerende constructies en partnerships met de bedrijfstak. Er lijkt in de politieke en regulerende beleidslijnen meer nadruk te liggen op medewerking van belanghebbenden dan op meer wetgevende activiteit – dit geldt niet alleen voor Europa, maar ook voor recente ontwikkelingen van de FCC in de Verenigde Staten. Tegelijkertijd is er behoefte aan een voortdurend herzien van de proportionaliteit van eventuele regulerende activiteit, zeker waar het sterk interventionistische maatregelen betreft (zoals "three strikes" of verplichte filtering) die fundamentele internetvrijheid en fundamentele consumentenrechten (bijvoorbeeld privacy) kunnen aantasten, en bestaande wettelijke zekerheden voor de sector ondermijnen.

Toch heeft de sector de kans zijn verantwoordelijkheden op dit gebied te vergroten met activiteiten om consumenten voor te lichten en middelen aan te bieden om hun vertrouwen in het gebruik van nieuwe online- en digitale diensten. In aanvulling op door de bedrijfstak aangevoerde initiatieven inzake corporate responsibility, is voor de handhaving meer samenwerking nodig binnen de sector en met overheids- en regulerende organen om een deugdelijke juridische basis te scheppen voor elk niveau van geplande interventie. Een voorbeeld vormen de verschillende niveaus van filteren en blokkeren van content – netwerkoperators zullen er zeker van willen zijn dat hun aansprakelijkheid is gedekt. Ook op het gebied van netwerkveiligheid kunnen er partnerships nodig zijn tussen publieke en particulieren instellingen om effectieve verzameling van vaak zeer gevoelige en vertrouwelijke gegevens te verzekeren als basis voor samenhangende en doeltreffende bestrijdingsstrategieën.

V. RISICO-/BATENANALYSE: DIGITAL CONFIDENCE LOONT DE MOEITE

In de vorige hoofdstukken is duidelijk geworden dat Digital Confidence een uitermate complex onderwerp is. Het is niet alleen een belangrijke "veilig-gevoel-factor" voor consumenten, maar Digital Confidence heeft ook relevante invloed op de economie. Online illegaal kopiëren heeft op het moment bijvoorbeeld een economische impact van enige miljarden euro's in Europa. Op elk gebied van Digital Confidence zijn er afwegingen te maken die allemaal hun sociale en economische impact hebben. Zo kan het zeer restrictief beschermen van de privacy van consumenten gevolgen hebben voor businessmodellen die gericht zijn op gericht en gepersonaliseerd adverteren – een substantiële bijdrage aan de Europese online advertentiemarkt van €57 miljard in 2012. Wij moeten ons realiseren dat al veel innovatieve onlinediensten als routeplanners en stadskaarten alleen gratis kunnen worden aangeboden omdat ze gefinancierd worden door reclame. Deze diensten kunnen onder druk komen te staan en nieuwe kunnen mogelijk niet worden gerealiseerd.

Ook moeten de verantwoordelijkheden en rollen binnen Digital Confidence die de diverse belanghebbenden in de digitale economie spelen duidelijk worden om een samenhangende aanpak te realiseren die waarde toevoegt aan de bedrijfstak en tevens voldoet aan de verwachtingen van de consument over de prestaties van de sector op alle gebieden van Digital Confidence. Deze rollen en verantwoordelijkheden dienen een eerlijke verdeling van de lasten te weerspiegelen en in proportie te zijn met de respectievelijke rollen van de belanghebbenden in de waardeketen. Als belangrijkste groei factoren zullen netwerkoperators, zowel dragers als leveranciers van internet en van de diensten over hun netwerken, zonder twijfel een centrale en belangrijke rol blijven spelen in het bevorderen van Digital Confidence: hun kernfunctie "doorgeefluik" staat onder aanzienlijke druk, net als de toekomstige waardeontwikkeling die grotendeels wordt bepaald door handel en diensten met toegevoegde waarde.

Zo leidt de "three strikes and you're out"-regel, waar contenteigenaren en hun partners voorstanders van zijn, ertoe dat netwerkproviders een rol krijgen in het monitoren en beoordelen van het gebruik van materiaal met copyright op hun netwerken. Deze aanpak kan de digitale economie, in het Verenigd Koninkrijk alleen al, jaarlijks £150 miljoen kosten – naast de implicaties voor de privacy van consumentengegevens.

Om te begrijpen wat de gevolgen zijn van het al dan niet slagen van Digital Confidence hebben we een holistische analyse uitgevoerd van de digitale economie en de opbrengsten ervan in Europa, nu en in de toekomst, om schattingen naar de gevolgen van een zwak en een sterk Digital Confidence in concrete getallen uit te drukken. Tot nu toe is er in studies en rapporten alleen gekeken naar de effecten van losse maatregelen met betrekking tot Digital Confidence, allemaal met verschillende uitgangspunten en voor verschillende geografische regio's. Voor onze schatting hebben we al deze input gebruikt en een consistent, holistisch model voor heel Europa en alle Digital Confidence-maatregelen gebouwd.

De risico-/batenanalyse biedt een begrijpelijk overzicht van de pijlers van Digital Confidence die de grootste financiële impact hebben. Het schat voor twee alternatieve scenario's de gevolgen op de inkomsten van de digitale economie in vergelijk met een standaardcase. Concreet laat het zien in welke mate de diverse inkomstenbronnen van de digitale economie gevaar lopen bij Digital Confidence-problemen en biedt de sector daarmee financiële aansporingen om zich te richten op oplossingen voor Digital Confidence. Met deze achtergrondkennis kunnen overheden initiatieven vanuit de sector ondersteunen op gebieden die eerder maatschappelijk dan financieel van belang zijn.

Het risico van het mislukken van een Digital Confidence is groot: een marktwaarde van €124 miljard in 2012 – 1 procent van het Europese BP – kan worden vernietigd.

Input voor deze analyse zijn een marktonderzoek opgebouwd uit een veelheid aan statistieken en verwachtingspatronen, afwegingen door deskundigen van Booz & Company op basis van bevindingen uit 50 gesprekken met experts in de sector en een diepteonderzoek naar best practices en vooruitzichten in de sector.

Gebaseerd op een diepgaand onderzoek van de verzamelde input, zijn de belangrijkste variabelen voor de analyse benoemd en gebruikt als vertrekpunt voor de modelontwikkeling. Het model is tot stand gekomen door herhaaldelijk een gevoeligheidsanalyse voor de diverse variabelen uit voeren. Het resultaat hiervan is samengevat in samenhangende scenario's die

nodig zijn om een geaggregeerd overzicht aan het licht te brengen over de voor- en nadelen van Digital Confidence.

1. FINANCIËLE SAMENVATTING: DE RISICO'S ROND DIGITAL CONFIDENCE ZIJN GROTER DAN DE POTENTIËLE BATEN

Als een referentie voor de analyse is de Europese[8)] digitale economie geschat op een inkomstenvolume van £436 miljoen als totaal voor toegang, commerce, content en adverteren in 2012, uitgaande van een gemiddelde jaarlijkse groei van 18 procent (2007-2012).

Het worst case-scenario – Digital Confidence mislukt, gedefinieerd als het "Industry Divergence"-scenario – laat grotere risico's zien dan de voordelen in het geslaagde scenario – het "One Direction"-scenario. Terwijl de risico's €78 miljard bedragen zijn de voordelen €46 miljard. Wanneer we die bedragen optellen, laat dat een verlies aan inkomsten van €124 miljard zien. Dit is het equivalent van 1 procent van het Europese BBP (bruto binnenlands product), met soortgelijke gevolgen voor investeringen en werkgelegenheid.

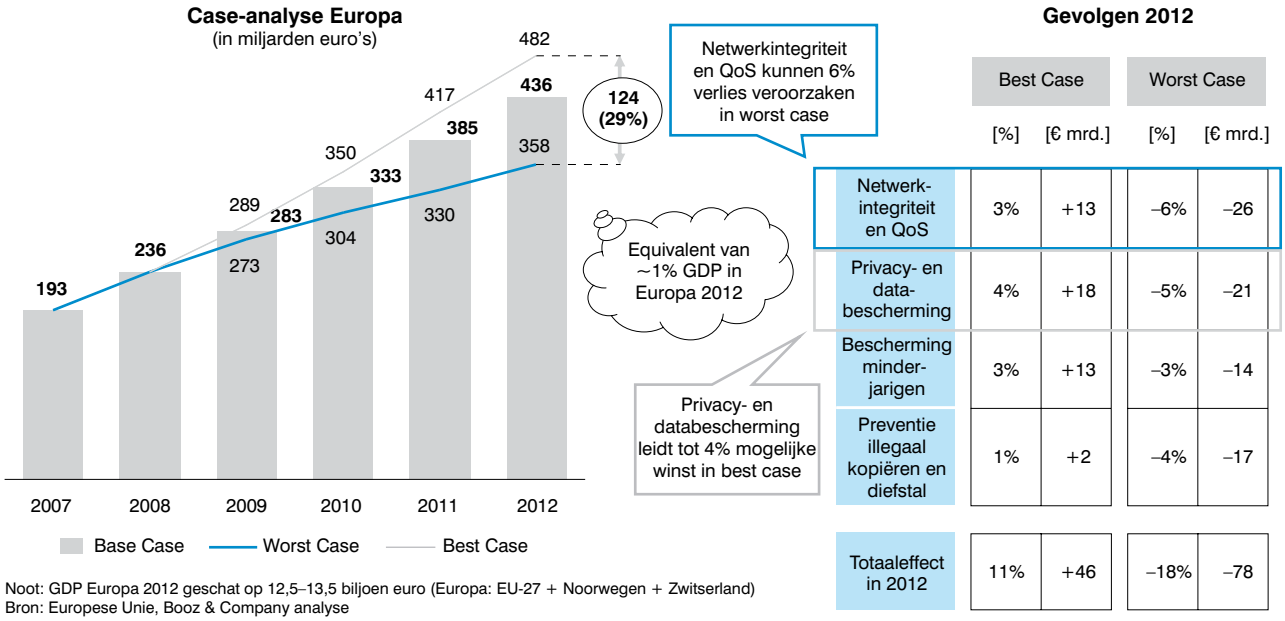
"Privacy- en databescherming" en "Netwerkintegriteit" en "Quality of Service" hebben een enorme invloed op de economie

De bedreigingen voor de inkomsten illustreren het potentiële waardeverlies voor het gehele ecosysteem van de digitale wereld; van consumenten tot adverteerders, en van contentproviders tot netwerkoperators. In het ergste geval zijn er minder gebruikers die minder doen en minder uitgeven dan in het beste geval. Hoewel de inkomsten niet helmaal verloren gaan (bijvoorbeeld verschuivingen van Amazon naar fysieke "echte" boekenwinkels), kunnen sommige businessmodellen en de daaruit voortvloeiende inkomsten totaal verloren gaan (onlineveilingen zijn bijvoorbeeld moeilijk te vervangen door offline veilingen).

Twee pijlers die dwars door alle soorten inkomsten snijden zullen de grootste financiele impact hebben. Als eerste is er Privacy- en Databescherming; dit heeft te maken met zorgen van de consument over de veiligheid van digitale data. Zo zullen consumenten in het worst case-scenario minder bereid zijn informatie te delen met derde partijen. Hierdoor komen innovatieve reclamemodellen waar de digitale sector en marketeers grote verwachtingen van hebben, onder zware druk te staan. Deze modellen vormen niet alleen het fundament van veel B2C-businessmodellen, maar bieden de consument ook voordelen, bijvoorbeeld betere voorlichting over aankopen die ze van plan zijn. Daar komt bij dat consumenten, uit angst voor de manier waarop wordt omgegaan met hun persoonlijke gegevens, minder gebruik zullen maken van e-commerce. Als tweede hebben Netwerkintegriteit en Quality of Service grote effecten op de inkomsten, omdat ze de digitale wereld ondersteunen door technologieplatforms te beschermen en te zorgen voor optimale verbindingen via het internet. Goed onderhouden kan het netwerk gebruikt worden om eindgebruikers te voorzien van meer bandbreedte en een QoS die alle gebruikers volledig laat genieten van het rijke digitale leven – van voice- en internetbrowsing tot multimediadiensten en video-on-demand. Hiermee beïnvloeden

8) In deze context staat Europa voor de EU-27 plus Noorwegen en Zwitserland.

Figuur 57: Invloed *Digital Confidence*



Noot: GDP Europa 2012 geschat op 12,5–13,5 biljoen euro (Europa: EU-27 + Noorwegen + Zwitserland)
Bron: Europese Unie, Booz & Company analyse

Netwerkintegriteit en Quality of Service direct het soort gebruik en het aantal gebruikers in alle belangrijkste inkomstencategorieën.

De andere pijlers onder Digital Confidence zijn belangrijk, maar hebben in puur economische termen minder impact omdat ze alleen doorwerken op bepaalde inkomsten. Preventie illegaal kopiëren en diefstal heeft vooral gevolgen voor de inkomsten van contenteigenaren. Daarbij komt het gevaar van een negatieve invloed op e-commerce als mensen overschakelen van online-aankopen naar traditionele informatiedragers als dvd's en cd's. Bescherming van minderjarigen heeft een indirect effect op het gebruik, als ouders bepalen hoe de kinderen het internet kunnen gebruiken en de kinderen zelf (doordat ze vaak gewaarschuwd zijn) afzien van het gebruik van bepaalde diensten, bijvoorbeeld sites voor sociaal netwerken.

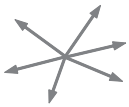
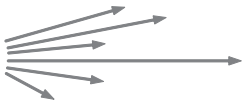
"De introductie van meer interactieve, bandbreedtevretende diensten is zeer sensitief voor Digital Confidence.

2. DIGITAL CONFIDENCE-SCENARIO'S – VAN DIVERGENTIE NAAR CONVERGENTIE

De scenario's die werden gebruikt om de impact van Digital Confidence te schetsen, zijn afgeleid uit kennisname van de problemen binnen de bedrijfstak en met name uit de casestudies die praktijken illustreren inzake de meest dringende problemen. De drie scenario's variëren in hun overkoepelende motto en kenmerken:

- "Business as usual" is het startpunt of de basisreferentie voor de analyse. Het scenario volgt het huidige verloop, met slechts enkele verbeteringen op bepaalde gebieden en maatregelen die min of meer synchroon verlopen bij alle belanghebbenden. Voorlichting gaat door op het huidige niveau; transparantie van gegevensgebruik wordt beter, maar er zijn geen aanzienlijke verbeteringen betreffende phishing en malware; doordat mitigatie tamelijk effectief is, is de QoS aanvaardbaar, al is er af en toe sprake van netwerkcongestie. De bescherming van content onder auteursrecht blijft in grote lijnen gelijk (schade door illegaal kopiëren blijft een feit).

Figuur 58: Invloed *Digital Confidence – overzicht mogelijke scenario*

	Worst Case Scenario	Base Case Scenario	Best Case Scenario
Motto	"Divergentie van de branche": Verschillende maatregelen getroffen 	"Business as usual": Maatregelen min of meer gelijklopend 	"Eén richting": Convergentie bij alle stakeholders 
Netwerkintegriteit en QOS	• Ongecoördineerd gebruik van het netwerk, wat leidt tot stelselmatige congestie en verslechterde gebruikerservaring	• Af en toe netwerkcongestie, met name tijdens piekuren, wat steeds meer dataverkeermanagement van service provider vraagt	• Significant meer bandbreedte dan vandaag en een betrouwbare, goede gebruikerservaring
Privacy- en databescherming	• Consumenten geven steeds meer data prijs, wat leidt tot profielrisico's	• Meer transparantie van datagebruik, maar geen significante verbetering van phishing en bedreiging identiteitdiefstal	• Educatie, transparantie en effectieve opt-in- en opt-out-mechanismes, wat leidt tot bereidheid data te delen (bijv. innovatieve reclame)
Bescherming minderjarigen	• Uiteenlopende educatieve inspanningen rond bedreigingen op het internet voor kinderen en ouders	• Voortzetting bestaande informatie- en filtermaatregelen met lichte procesverbeteringen	• Verbeterde en coherente informatie van ouders en minderjarigen door alle spelers • Meer gedisciplineerd gebruik door minderjarigen en sociale netwerken
Preventie illegaal kopiëren en diefstal	• Voortschrijdend illegaal kopiëren en afname van aanbod van beschikbare legale content	• Significant aandeel van illegale filesharing en downloaden van content met copyright	• Betere DRM-oplossingen voor traditionele businessmodellen
Situatie regelgever	• Biedt geen coherente visie, neigt tot overregulering (bijv. t.a.v. QoS- en databeschermingsvereisten)	• Richt zich in het algemeen op de grootste problemen, met name bij divergerende belangen (bijvoorbeeld bescherming minderjarigen en privacy), maar af en toe eenzijdige interventies als "Three Strikes"	• Draagt in hoge mate bij aan "één richting"-benadering, en stimuleert door de branche gestuurde regelgeving

• "Eén richting" is het beste geval wanneer de sector kiest voor een geharmoniseerde aanpak van Digital Confidence en alle spelers op een samenhangende manier werken aan een gemeenschappelijke visie. Voorlichting is als geheel beduidend beter, vaak in samenwerkingsverband tussen belanghebbenden; het vergrote bewustzijn van consumenten van de sterke en zwakke punten van gericht adverteren zorgt dat het werkt; door het gebruik van verscheidene aanvaarde maatregelen slagen netwerkoperators en serviceproviders erin zeer betrouwbare QoS te leveren, met hogere snelheden dan op dit moment. Onrechtmatige filesharing neemt af door toenemende bewustwording van de consument en nuttige contentaanbiedingen worden gekoppeld aan nieuwe, intelligente businessmodellen.

• "Sectordivergentie" is het meest nadelig voor de digitale economie, aangezien het verdere groei van de digitale wereld in de weg staat. In een dergelijke scenario opereren spelers onafhankelijk van elkaar, zonder gemeenschappelijke visie. Hierdoor worden uiteenlopende maatregelen toegepast, op inconsistente wijze. Maatregelen om minderjarigen in hun digitale omgeving te beschermen zijn beperkt in aantal en vaak tegenstrijdig. Consumenten ervaren problemen met hun privacy en worden sceptischer over de digitale wereld in het algemeen. Ongecontroleerd in dataverkeermanagement leidt vaak tot QoS-problemen en klachten over netneutraliteit. Problemen rond content onder auteursrecht groeien en een algemene "depressie" in de contentsector zorgen voor minder aanbod van legale content in de digitale wereld.

Bijna €80 miljard aan e-commerce-opbrengsten staat in 2012 op het spel in relatie met Digital Confidence.

Het grootste verschil tussen de scenario's zit in de mate waarin spelers in de bedrijfstak op één lijn zitten in de aanpak van Digital Confidence. Eenduidigheid betekent niet noodzakelijkerwijs dat spelers alles op dezelfde manier doen; het gaat meer om de mate van overeenstemming in de gehele sector om dezelfde richting te volgen. Het gaat om de mate waarin er een gemeenschappelijk begrip bestaat van een dergelijke richting en de prioriteiten in het algemeen, zowel als de daaruit voortvloeiende consequenties voor elk van de belanghebbenden.

Een grotere mate van gedeelde verantwoordelijkheid leidt – in het beste geval – tot verbetering in het bewerkstelligen van Digital Confidence binnen alle pijlers, levert een positieve bijdrage aan het gebruik en doet daardoor de opbrengsten toenemen.

3. VOORNAAMSTE FINANCIËLE AANDRIJVERS: DIGITAL CONFIDENCE HEEFT DE MEESTE INVLOED OP RECLAME EN CONTENT

De inkomstencategorieën die het meest afhankelijk zijn van Digital Confidence zijn content en reclame.

Content is zeer gevoelig voor de mate van Digital Confidence. Dit wordt nu al duidelijk door bijvoorbeeld de financiële gevolgen van illegaal kopiëren van video – off- en online. Voor 2007 verwacht de Motion Picture Association of America (MPAA) door illegaal kopiëren een wereldwijd verlies van meer dan $18 miljard; dat betreft de directe schade en laat de mogelijke indirecte economische impact nog buiten beschouwing. Als er 31 procent van de opbrengsten op het spel staat in het slechtste geval van Digital Confidence, moeten bedrijven en consumenten erop vertrouwen dat online-contentplatforms ten dienste staan van contenteigenaren en een veilige, risicoloze omgeving zijn voor persoonlijke gegevens van gebruikers (bijvoorbeeld gebruikshistorie, creditcardgegevens, etc.). Verder is content vaak afhankelijk van realtime levering (zoals iPlayer van de BBC en andere oplossingen voor streaming video-on-demand) en dus sterk afhankelijk van de onderliggende netwerkinfrastructuur. De groei van opbrengsten en groei van content is afhankelijk van de kwaliteit van het netwerk geleverd door de netwerkoperators. Netwerk- en contentproviders moeten tot een model komen dat kosten en baten gelijk verdeelt zodat de juiste stimulans ontstaat om te investeren in de infrastructuur, noodzakelijk om van het internet een medium te maken dat content voor de massamarkt levert. In het beste geval is €4 miljard extra opbrengsten haalbaar, vergeleken met een mogelijk verlies van €6 miljard.

e-Commerce, content, en reclame zijn het meest blootgesteld aan risico's door een gebrek aan Digital Confidence.

Reclame is ook in hoge mate afhankelijk van het consumentenvertrouwen. Adverteerders gaan immers alleen door met meer digitale dan traditionele reclame maken als de groei in online bestede tijd doorzet. Voor reclame is het best mogelijke scenario €9 miljard winst en het slechtste €14 miljard verlies. Dit betekent dat bijna 25 procent van advertentieopbrengsten op het spel staat in het worst case-scenario.

Absoluut gezien is e-commerce het meest afhankelijk van Digital Confidence, omdat het verreweg de grootste inkomstencategorie is. Het slechtst mogelijke resultaat komt uit op een

verlies €52 miljard, het beste op de helft daarvan, relatief gezien. Toch wordt e-commerce minder getroffen, omdat het vertrouwen in gevestigde spelers (zoals Amazon) al tamelijk groot is. De goederen worden fysiek afgeleverd en de feitelijke invulling van de dienst is daarmee niet afhankelijk van het internet.

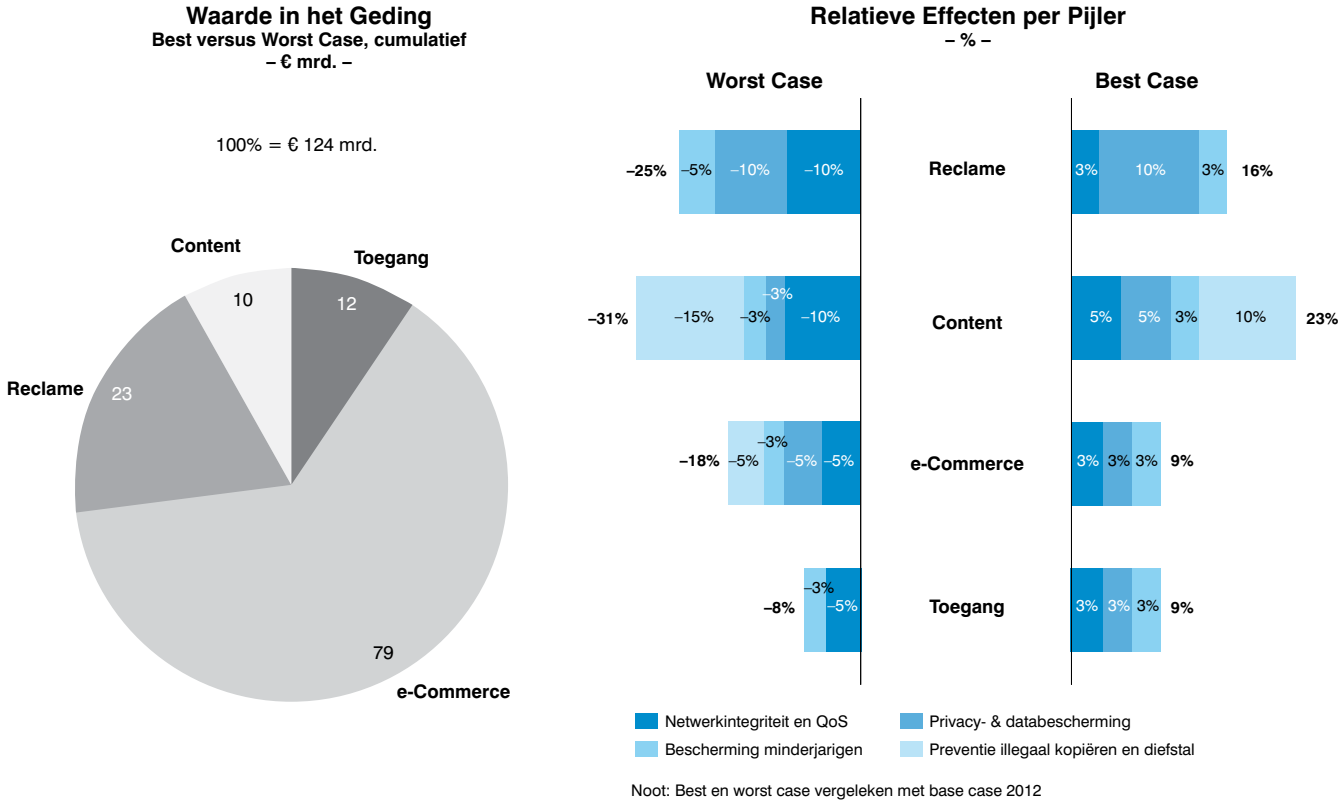
Als onderliggende inkomstencategorie wordt internettoegang het minst beïnvloed door Digital Confidence. Het wordt steeds meer als gebruiksproduct gezien en de groeiverwachtingen zijn gering. Succes dan wel mislukking van Digital Confidence zal het aantal gebruikers waarschijnlijk niet beïnvloeden. Het beste en het slechtst mogelijke resultaat zijn beide €6 miljard. Figuur 58 vat het beste en het slechtste geval samen.

4. CONCLUSIE

Louter economisch gezien en zonder het bredere maatschappelijk aspect in acht te nemen, toont de risico-/batenanalyse aan dat de digitale bedrijfstak een belangrijke impuls voor de economie kan zijn. Hiertoe dienen bepaalde gebieden van Digital Confidence op een samenhangende manier te worden aangepakt om ten minste de worst case-scenario's voor de opbrengsten te vermijden en idealiter te streven naar de best mogelijke opbrengsten. In de eerste plaats is Privacy- en Databescherming financieel belangrijk, vooral, maar niet beperkt tot, de implicaties ervan voor businessmodellen op het gebied van innovatieve (gerichte) reclame. In de tweede plaats zijn Netwerkintegriteit en Quality of Service vereist ter ondersteuning van de voortdurende groei van content- en videoservices. In de derde plaats is het segment Preventie illegaal kopiëren en diefstal relevant voor zowel contenteigenaren als voor e-commerce. Naast de duidelijke opbrengstimplicaties voor de contentsector in het beschermen van de bestaande waarde van hun rechtenportfolio's en het introduceren van innovatieve digitale en onlinebusinessmodellen, bestaat er een aanzienlijk risico in verband met de negatieve invloed op e-commerce-transacties doordat mensen offline producten gaan kopen, waartoe nieuwe businessmodellen (zoals online-veilingen) geen mogelijkheid bieden.

Kortom, netwerkproviders moeten een belangrijke rol blijven spelen, aangezien hun kernactiviteit in hoge mate bepalend is voor het succes van de aandrijvers van de economische groei. De mate van netwerkintegriteit heeft een grote economische invloed, zelfs al lijkt hun eigen kernactiviteit het minst blootgesteld aan de voordelen/risico's van het slagen of mislukken van Digital Confidence.

Figuur 59: *Invloed Digital Confidence – groeigebieden en -pijlers*



VI. FRAMEWORK FOR ACTION

1. BELEID EN PROCEDURES

Europa's digitale economie heeft een sterk groeiperspectief, aangedreven door diensten van het Web 2.0-type die gemeengoed zijn geworden door het gebruik van de functies en toegenomen capaciteit van bijna overal beschikbare breedbandnetwerken. Migratie naar Next Generation toegangsnetwerken, toegenomen gebruik van geraffineerde netwerktechnologieën en de nieuwe generatie steeds assertievere "born digital" -consumenten zijn mogelijk ontwrichtende krachten voor het digitale economische ecosysteem. Dit nieuwe paradigma is een aanzienlijke uitdaging voor zowel beleidsvormers en regelgevers als voor de sector in het algemeen. De mate waarin consumenten vertrouwen hebben in de manier van zakendoen en het bieden van veilige diensten en netwerkomgevingen van providers van diensten en platforms, alsmede in het vermogen van overheden en regelgevende instanties om standaarden voor consumentenbescherming toe te passen, wordt in snel tempo een belangrijk invloed op de potentiële groei van de digitale economie.

De sector bevindt zich in een bepalende fase in de verdere ontwikkeling van de digitale wereld. De risico-/batenanalyse laat de financiële invloed van Digital Confidence op de sector zien. Financieel gezien is er een duidelijke noodzaak voor actie; in de sector als geheel staat €124 miljard op het spel. Naast deze financiële redenen is het opbouwen van digitaal vertrouwen echter ook een maatschappelijke verantwoordelijkheid. Het gaat immers zowel de consument als de regelgevers en de maatschappij als geheel aan.

De casestudies in dit rapport bevestigen dat diverse belanghebbenden in de bedrijfstak zich momenteel bezighouden met de materie. Toch gaat het hierbij in veel gevallen om reacties op protesten van het publiek, of onder druk van de media en regelgevers. Sprake is dan van ingrijpende voorvallen, waarbij veiligheid, privacy of andere vertrouwensbreuken in het spel zijn. Vertrouwensbreuken ontstonden tot nu toe door onder meer:

- Niet voldoen aan verwachtingen wat betreft het serviceniveau, bijvoorbeeld een te hoog prestatieniveau beloven waar de netwerkoperator dit niet kan waarmaken. Dit gebeurde in de Verenigde Staten toen ISP's bekendmaakten dat via hun netwerken toegang tot kinderpornografie onmogelijk zou zijn. Een ander voorbeeld is de situatie waarbij gebruikers een verslechtering constateerden van populaire, veel bandbreedte vereisende diensten zoals P2P-sites, door de toepassing van netwerkmanagementtechnieken.

- Niet voldoen aan verwachtingen rond de effectiviteit van filteren in het geval van kinderpornografie.

- Het gebruik van vergaande technieken voor internetmonitoring voor commerciële doeleinden

Vanuit het perspectief van consumentenaanvaarding komen, ondanks de complexiteit en diversiteit van de huidige wijzen van aanpak, meerdere richtlijnen voor best practices bovendrijven:

- Consumenten accepteren handelswijzen die transparant en niet opdringerig zijn – netwerkproviders alsmede content- en platformspelers dienen, samen met de regelgever, dit soort communicatie te stimuleren.

- Consumenten zijn bezorgd over de manier waarop ISP's en netwerkoperators digitale klantgegevens beheren – eenduidige verklaringen en een consistent en betrouwbaar raamwerk voor regelgeving moeten hierbij de hoogste prioriteit krijgen.

- Consumenten eisen inzicht in de risico's die ze lopen – dit vraagt om toegang tot de geschikte hulpmiddelen, opt-in-/opt-out-mogelijkheden en voorlichting.

- Consumenten accepteren maatregelen die Quality of Service garanderen. Als hiervoor actief dataverkeermanagement nodig is, staan ze daarvoor open, vooropgesteld dat er openlijk bericht wordt over service en er sprake is van zowel eerlijke en transparante tarieven als niet-discriminerende toegang.

De casestudies laten ook zien hoe ingewikkeld het is om Digital Confidence te laten slagen. Zelfs de best bedoelde oplossingen, gericht op

het voorkomen van bepaald gedrag door content te blokkeren of te filteren, kunnen in strijd zijn met burgerlijke vrijheden en vereisten op het gebied van netneutraliteit. Oplossingen die zich richten op voorlichting en bewustmaking van de consument van de risico's en verantwoordelijkheden vereisen een hoge mate van betrokkenheid van de sector om te bouwen aan die bewustwording.

De software ter ondersteuning van beide benaderingen is beschikbaar, maar een gemeenschappelijke definitie van standaarden en beleid ten aanzien van ongepaste content is nog steeds nodig.

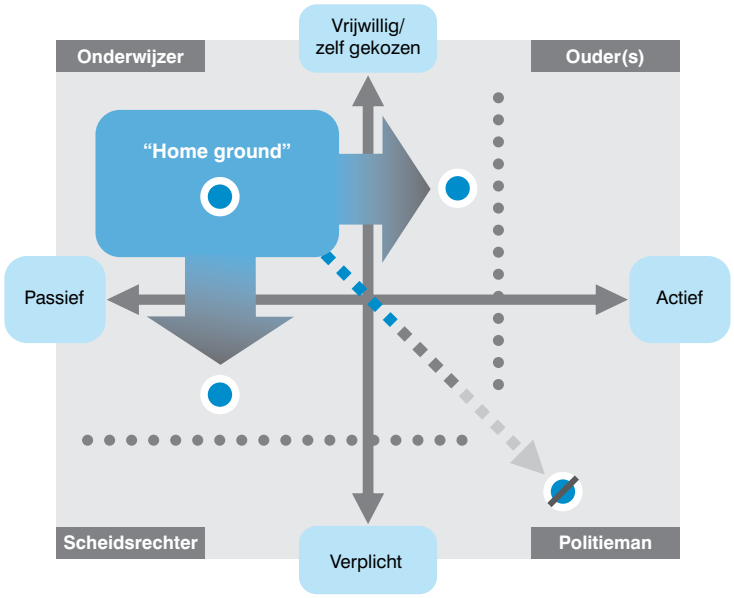
Om te voorkomen dat antwoorden op Digital Confidence-problemen, die steeds groter worden en een globaal karakter krijgen, verspreid en gefragmenteerd raken, riepen we op tot een holistische aanpak en eenduidige afstemming in de gehele sector. Dit zal uiteindelijk leiden tot meer transparantie en de gebruiker de weg wijzen rond de risico's en baten van de digitale wereld.

Alle vier de pijlers van Digital Confidence moeten benut worden om de groei van de digitale wereld door te zetten.

Elk van de Digital Confidence-pijlers heeft een complex karakter waar het gaat om de bedreigingen en oplossingen alsmede de diverse posities en belangen van de belanghebbende.

De kwestie wordt hoofdzakelijk beschouwd vanuit het perspectief van de kabeloperator. Diens aanbevolen positie ten aanzien van Digital Confidence is gedefinieerd en in lijn daarmee zijn gepaste maatregelen in detail beschreven. Vervolgens komt de bespreking op sectorniveau door de implicaties voor andere belanghebbenden, en met name de regelgevers, in kaart te brengen.

Figuur 60: *Positionering: de "Home Ground" van internet providers*



2. NETWERKOPERATORS EN ISP'S MOETEN EEN DUIDELIJKE POSITIE INNEMEN TEN AANZIEN VAN DIGITAL CONFIDENCE

Het beeld dat netwerkproviders en ISP's van zichzelf hebben speelt een belangrijke rol bij het bepalen van de mate van betrokkenheid bij het vaststellen van Digital Confidence-beleid. Zijn we "slechts een doorgeefluik" – plaveien en onderhouden we alleen de snelwegen? Of maken we de gedragsregels voor het reizen op die snelwegen en vertalen we dat in beleid?

Er is evenwel geen eenvoudig antwoord – de positie die een netwerkoperator of ISP inneemt varieert in de pijlers van Digital Confidence.

Het Digital Confidence Positioneringmodel is een constructie om de positie te bepalen van individuele Digital Confidence-pijlers én van alle tezamen. De verticale as differentieert de onderliggende principes, met "vrijwillig" en "verplicht" als de twee polen. De horizontale as differentieert hoe maatregelen worden getroffen – passief op een "hands-off"-manier, of actief volgens een "volledig beheer"-benadering. De vier kwadranten die dit oplevert kunnen symbolisch verbonden worden met archetypes van maatschappelijke rollen. De onderwijzer geeft gebruikers zoveel mogelijk informatie over kansen en bedreigingen, maar zal doorgaans niet actief corrigerend optreden. De ouder informeert gebruikers over bedreigingen en maatregelen zoals de onderwijzer, maar treedt zo nodig proactief op. De scheidsrechter baseert zich van geval tot geval op zichzelf opgelegde handhaving van regels en richtlijnen, eerder dan op voorlichting, maar de regels zijn gebaseerd op wederzijdse instemming. De politieagent is van nature geneigd wetgeving strikt na te leven en alle daartoe noodzakelijke maatregelen te nemen, en doet dat op basis van strikte regels, zoals alle onwettige activiteiten blokkeren.

Op basis van ons onderzoek en kennis van de sector en de vele gesprekken die we voerden, is het duidelijk dat de natuurlijke "thuisbasis" voor de ISP tot nu toe de kwadrant linksboven is – De Onderwijzerrol. De karakteristieken van deze kwadrant zijn in lijn met het oorspronkelijke zelfbeeld van een netwerkoperator: het doel van zijn kernactiviteit was en is nog steeds het leveren van een veilig, betrouwbaar en krachtig netwerk voor internetverkeer, zonder zich te bemoeien met wat er op dat netwerk gebeurt.

Hieruit kan een opvoedkundige rol worden afgeleid om consumenten bewust te maken van problemen rond digitaal vertrouwen en ze hulpmiddelen aan te reiken om er op een "hands-off"-manier mee om te gaan. Een zodanige positionering beperkt risico's en aansprakelijkheden wat betreft zaken waar de ISP in principe niet verantwoordelijk voor is. In het algemeen zou de ISP niet verantwoordelijk zijn voor het opstellen van Digital Confidence-standaarden, bijvoorbeeld door copyrightschending te vervolgen. Onze analyse toont echter ook aan dat dit niet volstaat. Een aanzienlijk deel van toekomstige groei houdt verband met meer gebruik van bestaande en nieuwe digitale, online-diensten met toegevoegde waarde. Hierbij wordt de mate waarin consumenten vertrouwen hebben in hun provider een belangrijke voorwaarde voor groei en succes van de digitale markt. Als ISP alle kaarten inzetten op voorlichting, corporate responsibility programma's en opereren volgens de wet, is dat niet voldoende om klantaanvaarding te bewerkstelligen en vertrouwen op te bouwen. Wetgeving kan de snelheid, reikwijdte en schaal van veranderingen vaak niet bijhouden. Voorbeeld hiervan zijn nieuwe technieken voor dataverkeermonitoring en toegenomen veiligheidsrisico's door geraffineerde cybermisdaad, die van invloed zijn op Digital Confidence. Vandaar dat succesvolle bedrijven meer doen dan alleen de regels volgen; ze nemen een voorsprong op de ontwikkelingen door Digital Confidence als volgt te stimuleren:

- Ze nemen besluitvormingsprocedures en protocollen op in hun beleid met het oog op het opbouwen van vertrouwen.

- Ze zijn zo open en transparant mogelijk in hun communicatie met consumenten.

- Ze doen meer moeite om hun klanten goed te informeren en in staat te stellen hun belangen in de digitale wereld zelf te beschermen.

- Ze maken gebruik van een gefaseerde, proactieve benadering conform het E3-paradigma: Educate eerst, Empower vervolgens en Enforce waar nodig.

Op deze manier moeten netwerkoperators proactief vormgeven aan de toekomstige ontwikkelingen binnen de bedrijfstak, door oplossingen en benaderingswijzen te ontwikkelen die onontkoombaar zullen leiden tot nieuwe posities in zowel de rol van Ouder als die van Scheidsrechter. Er is een aantal redenen waarom netwerkoperators en ISP's buiten hun "thuisbasis" moeten treden.

Ten eerste kunnen sterke strategische of bedrijfsmotieven ertoe leiden dat de netwerkoperator of ISP zijn "thuisbasis" verlaat, bijvoorbeeld om zeker te zijn van de goodwill van de consument. Zo zullen ouders hun kinderen het internet vaker laten gebruiken als ze tevreden zijn over de mate van bescherming. Dataverkeermanagement is eveneens van strategische waarde; het zorgt ervoor dat niet alleen de zware gebruikers maar alle consumenten profiteren van investeringen in Next Generation toegangsnetwerken en grotere bandbreedtes. In hoeverre een netwerkoperator in staat is Quality of Service en optimale breedbandervaring te garanderen, is ook afhankelijk van de concurrentie en mede bepalend voor de toekomstige infrastructuur.

De industrie zou het E³ paradigma moeten gebruiken: Educate, Empower, Enforce.

Ten tweede kan mogelijk buitenproportionele interventie door regelgevers overbodig worden door betere regulering en samenwerking binnen de sector zelf te stimuleren. Goed voorbeeld hiervan is Groot-Brittannië, waar aangekondigd werd dat toonaangevende ISP's gaan samenwerken met de British Phonographic Industry om klanten actief te benaderen en te waarschuwen tegen illegaal kopiëren. In de Verenigde Staten is Comcast het op constructieve wijze eens geworden met BitTorrent om te komen tot dataverkeermanagementbeleid waarin beide partijen zich kunnen vinden.

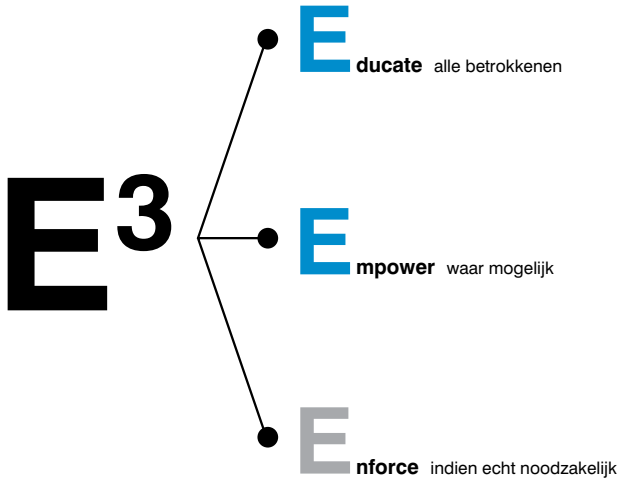
Toch moeten ISP's erg voorzichtig zijn met het aannemen van een rol die niet tot hun primaire verantwoordelijkheid behoort. Als ze iets ondernemen dat hun veilige haven van "slechts een doorgeefluik" ondermijnt en te maken krijgen met onoverzienbare aansprakelijkheden, zal dat de Digital Confidence niet ten goede komen – en de verwachtingen van het publiek zullen dan al gestegen zijn. Bovendien zou dat negatieve signalen richting investeerders en aandeelhouders betekenen.

Tenzij ze er wettelijk toe verplicht worden, zouden ISP's in elk geval niet de rol van Politieman op zich moeten nemen. Deze rol staat voor een zeer dwingende benadering, met een negatieve invloed op de consumentenacceptatie. Indien ze er wettelijk toe worden verplicht, moeten netwerkoperators en ISP's die rol niet alleen daadwerkelijk op zich nemen, maar zijn ze ook beschermd tegen juridische aansprakelijkheden. Als ze bijvoorbeeld wettelijk verplicht worden bepaalde internetsites te blokkeren – vanwege bezorgdheid om de content – lopen ze minder

risico op beschuldigingen van schending van auteursrecht, burgerlijke vrijheden, vrijheid van meningsuiting en netneutraliteit.

Samengevat vertaalt deze positionering zich in een duidelijk paradigma: E3 – Educate, Empower, Enforce. De positie in de matrix bepaalt de mate waarin deze rollen toegepast worden in het geval van de netwerkoperator.

Figuur 61: *Het E^3 paradigma*



3. CALL FOR ACTION VOOR DE NETWERKOPERATOR: DE VIJF BELANGRIJKSTE INITIATIEVEN VOOR DIGITAL CONFIDENCE

Het E3-paradigma maakt kort en bondig duidelijk wat een netwerkoperator of ISP te doen staat, maar is net zo goed van toepassing op alle andere belanghebbenden binnen de digitale wereld.

Educate. Netwerkoperators en ISP's moeten er zeker van zijn dat hun klanten de bedreigingen rond de digitale wereld begrijpen en ze van de kennis voorzien om er op de juiste wijze mee om te gaan, zodat ze veilig te werk kunnen gaan. Beleid moet duidelijk en transparant zijn voor de eindgebruikers. Transparantie over het bedrijfsbeleid met betrekking tot Digital Confidence dient hiervan deel uit te maken.

Empower. Netwerkoperators en ISP's moeten hun klanten in staat stellen zelf het beheer te hebben over digitale bedreigingen en problemen, bijvoorbeeld middels een opt-in- of opt-out-voorziening om ongewenste content te blokkeren. Meer in het bijzonder moeten netwerkoperators en ISP's hun klanten voorzien van zulke processen en tools, en derde partijen helpen bij het ontwikkelen van deze tools en diensten.

Enforce. Netwerkoperators en ISP's moeten proactief optreden en richting geven aan het gebruikersgedrag als het algemeen belang om Digital Confidence te beschermen in het geding is. In dat geval dienen ISP's sectorbreed de neuzen in dezelfde richting te krijgen en best practices te delen.

Door sterk de nadruk te leggen op voorlichting en klanten zelf middelen in handen te geven, verandert hun zelfbeeld en de manier waarop ze informatie tot zich nemen en problemen oppakken. Een recente studie (de Trust Barometer van Edelman 2008) van Europese "Info-entials", jonge opiniemakers tussen 25 en 35 jaar, wees uit dat zij op een heel andere manier informatie vergaren dan hun voorgangers; ze gebruiken uiteenlopende informatiebronnen en vormen hun mening door voortdurend participeren, heroverwegen en delen. Ze staan open voor – of eisen zelfs – deugdelijke voorlichting en middelen om zelf te kunnen optreden. Het onderzoek komt tot de conclusie dat ze – hoewel ze "traditioneel cynisch tegenover de zakenwereld" staan– er vandaag de dag toch verhoudingsgewijs meer vertrouwen in krijgen. Maar de betrouwbaarste informatiebron voor Info-entials in de meeste EU-landen zijn "mensen zoals jij en ik", en NGO's.

Netwerkoperators en ISP's kunnen hierop voortbouwen, niet alleen om Digital Confidence-zorgen weg te nemen, maar ook om het te gebruiken als een bijdrage aan de traditionele klantenbinding.

Met deze algemene richtlijn als uitgangspunt wordt vanuit ondernemingsgericht perspectief concrete maatregelen geformuleerd. Deze maatregelen zijn verdeeld over vijf initiatiefgebieden:

1. BELEID

Netwerkoperators en ISP's dienen een duidelijke positionering vast te stellen ten aanzien van Digital Confidence met hun strategie en positie voor elke vertrouwenspijler. Dit moet de basis zijn voor al het beleid inzake Digital Confidence op vier gebieden: Bescherming van minderjarigen, Data- en Privacybescherming, Dataverkeermanagement en illegaal kopiëren. Hun positiestatement moet gedetailleerd genoeg zijn om concreet inzicht te geven in de onderliggende vragen in verband met deze kwesties, dat wil zeggen, hoe wordt het evenwicht afgewogen tussen ongepaste content en vrijheid van meningsuiting?

Als volgende stap moet dit beleid worden ingebed in de kernprocedures van het bedrijf. In de meeste gevallen zal dit van directe invloed zijn op de manier waarop netwerkoperators

denken over productontwikkeling, bijvoorbeeld door te zorgen dat alle aangeboden producten en diensten voldoen aan de normen.
Daarnaast moeten netwerkoperators hun Digital Confidence-beleid en -procedures actueel houden, door bestaand beleid en procedures regelmatig te controleren op juridische aspecten, openbaar beleid en techniek.

Niet in de laatste plaats wijzen de in dit rapport geanalyseerde cases naar een belangrijke les: Digital Confidence vereist vertrouwen, en de beste basis voor vertrouwen is open communicatie; transparantie loont. Bedrijven zouden dan ook open moeten zijn over het beleid dat ze hanteren en de beweegredenen ervan, inclusief de zakelijke. De ervaring leert dat consumentenaanvaarding in het algemeen groot is als regels en de onderliggende beweegreden openlijk worden besproken, zoals bijvoorbeeld de gerichte reclame van Google's Gmail laat zien. Dit maakt tevens een dialoog met de consument mogelijk, wat zeer nuttig kan zijn om oplossingen te verbeteren.

2. GOVERNANCE

Kwesties rond Digital Confidence zijn complex, zeer gevoelig en beïnvloeden elkaar wederzijds. Vaak vereisen ze dat een bedrijf fundamentele principes hanteert, bijvoorbeeld: hoe gaan we om gaan met content met seksueel misbruik? Als dat verkeerd gebeurt, brengt dat aanzienlijke financiële en reputatierisico's met zich mee. Daarom is het uiterst belangrijk dat het topmanagement hier voldoende aandacht aan schenkt. Digital Confidence moet op een duidelijke manier worden ingebed in de organisatiestructuur door bijvoorbeeld een stuurcommissie met senior toezicht en voldoende bevoegdheid om de vereiste activiteiten te implementeren.

3. TECHNOLOGIE

Voor Digital Confidence vereiste technologieën zijn op grote schaal voorhanden. De aandacht richt zich nu vooral op het beslissen over individuele positionering, het vaststellen van passend beleid en het creëren van ondersteunende governance-structuren. Toch moet er door de meerderheid van de netwerkoperators geïnvesteerd worden in bepaalde technologieën ter voorbereiding op de toekomst. Het gaat daarbij om het handhaven van de Quality of Service gezien het toenemende multimediadataverkeer. Netwerkoperators zullen hierover moeten beslissen door een afweging te maken tussen het toevoegen van transportcapaciteit en actief dataverkeermanagement. Dit kan tevens gerealiseerd worden middels gefaseerde tarieven. Verder dienen ze samen te werken met contentproviders om hun netwerken te optimaliseren voor het doorgeven van multimediacontent, zoals peer-to-peer-caches (bijvoorbeeld het P4P-initiatief) of contentnetwerken.

Ze moeten regelgevers laten weten dat ze het probleem op de juiste manier aanpakken.

Een ander groot technologisch risico wordt gevormd door de apparatuur van de eindgebruiker. Die is in de meeste gevallen niet voldoende beschermd tegen bedreigingen zoals virussen, botnets en andere vormen van malware. Softwareoplossingen bestaan al wel, maar netwerkoperators en ISP's moeten hun klanten nog actiever aanmoedigen om deze oplossingen daadwerkelijk te gebruiken. Netwerkoperators en ISP's moeten bovendien hulpmiddelen en oplossingen inzetten die de consumenten in staat stellen controle te houden over het risico dat ze lopen. Dit kan bijvoorbeeld middels opt-in-/opt-out -methodes. Dit vereist wel dat er meer actie wordt ondernomen. Het aanbieden van oplossingen die van de website gedownload kunnen worden, is niet genoeg: ISP's moeten programma's hebben die het aantal geïnstalleerde oplossingen in de gaten houden (waardoor hun onderwijzerrol feitelijk het karakter krijgt van de "ouder"-positie).

4. CONSUMENTENVOORLICHTING

Kabel- en telecom netwerkoperators en ISP's moeten zich samen met NGO's richten op programma's voor de sector en zelf initiatieven nemen voor passende voorlichting (bijvoorbeeld voorlichtingscampagnes op hun eigen websites).

Deze programma's moeten bedreigingen bespreken op het gebied van datapublicatie, gericht adverteren, illegaal kopiëren en online-gedrag in het algemeen (waaronder ook pesten, uitlokking en onaanvaardbare content).

Voorlichting moet gericht plaatsvinden, afgestemd op specifieke gebruikersgroepen, inclusief ouders en kinderen. Het programma voor ouders moet gericht zijn op de manier waarop zij de activiteit van hun kinderen te kunnen controleren en hen bewust kunnen maken van de gevaren van het internet en hen de hulpmiddelen leren kennen om dit te verwezenlijken. Bij het voorlichten van kinderen moet het herkennen van gevaren en hoe ermee om te gaan, centraal staan.

5. REGULERING

Netwerkoperators moeten regelgevers aanmoedigen om zich op specifieke actiegebieden te richten en bij te dragen aan de inspanningen van

de bedrijfstak om proactief vertrouwen op te bouwen, daar waar de netwerkoperator of ISP geen invloed uitoefent (zoals het opstellen van zwarte lijsten met illegale content of de wetshandhaving). Regelgevers moeten ervoor waken al te proactief regels op te stellen op deze gebieden, tenzij ze er zeker van zijn dat het in juiste mate gebeurt. De regelgever hoeft alleen direct betrokken te worden als consumentenbelangen daadwerkelijk gevaar lopen.

Hierop inhakend dient de sector duidelijk te laten zien dat ze Digital Confidence serieus neemt door het initiatief te nemen tot de ontwikkeling van samenhangende oplossingen. Bij zulke oplossingen moeten alle spelers betrokken zijn en de implementatiekosten en latere financiële beloningen dienen evenredig te worden verdeeld. Regelgevers moeten de bedrijfstak de ruimte geven om dergelijke oplossingen te ontwikkelen en zowel samenwerking met de belanghebbende als financiële supportprogramma's stimuleren. Daarbij dienen ze concurrentieaspecten in het voordeel van de consument te laten werken, liever dan regelgeving toe te passen. Hoewel goed bedoeld, kan regelgeving vanuit de consument gezien contraproductief zijn en economische schade aanrichten.

Bij het uitvoeren van maatregelen in al deze vijf initiatiefgebieden kunnen netwerkoperators en ISP's het beste zoveel mogelijk samenwerken met NGO's. Veel aspecten kunnen veel effectiever worden aangepakt als een operator samen met een NGO het initiatief neemt; de NGO kan netneutraliteit en sectorbrede inzetbaarheid waarborgen, gebruikmakend van de goede reputatie van NGO's. Recente studies laten zien dat consumenten veel vertrouwen in NGO's hebben.

4. IMPLICATIES VOOR ANDERE BELANGHEBBENDEN

Deze positie van de netwerkoperator maakt ook de verwachtingen ten aanzien van andere belanghebbenden in het ecosysteem van de digitale wereld duidelijk. De twee belangrijkste groepen zijn:

- Consumenten
- Andere leveranciers in de digitale waardeketen, zoals contentproviders, software- en toepassingontwikkelaars, en distributeurs (bijvoorbeeld e-shops)

CONSUMENTEN

Consumenten moeten overtuigd worden van de noodzaak van gezond verstand in de digitale wereld, net als in de offline wereld. Bovendien moeten ze leren omgaan met de op de consument gerichte oplossingen die netwerkoperators, ISP's en anderen ontwikkelen, waarmee ze zelf de gevaren van de digitale wereld kunnen beheren en beheersen. Om dat te leren moeten ze voorlichting door openbare instanties (zoals scholen, universiteiten en overheidsinstellingen) aannemen en gebruiken.

Consumenten moeten gebruik leren maken van de hulpmiddelen die de bedrijfstak ze aanreikt.

LEVERANCIERS VAN AUTEURSRECHTELIJK BESCHERMDE CONTENT HEBBEN TWEE MANIEREN OM HUN DOEL TE BEREIKEN

Contenteigenaren moeten ervoor zorgen dat hun content onder auteursrecht voldoende is beschermd. De muziekssector heeft enige tijd geworsteld met het ontwikkelen van businessmodellen die de nodige controle-instrumenten bevatten om illegaal kopiëren te voorkomen. Het probleem speelt nu ook in de film- en televisiesector door de beschikbaarheid van grotere bandbreedtes en compressietechnieken. Contenteigenaren moeten gezamenlijk oplossingen ontwikkelen om de content die ze bezitten op eerlijke wijze te gelde te maken. Om dit te bereiken, moeten er op sectorniveau oplossingen worden ontwikkeld voor copyrightbescherming. Spelers in de contentsector kunnen niet uitsluitend vertrouwen op contentbescherming door netwerkoperators. Bovendien accepteren consumenten niet zo snel oplossingen van internet- en netwerkspelers (zoals filteren of blokkeren van content) als dat louter om commerciële redenen gebeurt. Dat geldt ook voor bescherming tegen illegaal kopiëren, maar niet als er morele of sociale aspecten meespelen (bijvoorbeeld het blokkeren van kinderpornografie). Oplossingen voor illegaal kopiëren moeten zowel innovatieve businessmodellen omvatten, als managementtechnieken voor digitale rechten ondersteunen.

ANDERE DERDE PARTIJEN DIENEN SAMEN TE WERKEN MET DE INTERNETSECTOR

e-Commerce-bedrijven moeten samen met operators en ISP's werken aan gezamenlijke voorlichtingsprogramma's rond onderwerpen van wederzijds belang (bijvoorbeeld phishing). De bedoeling van dergelijke programma's moet zijn het consumentenvertrouwen te verbeteren door betere kennis van de bedreigingen en problemen. Ook moeten consumenten de hulpmiddelen krijgen om deze risico's te beheersen. Netwerkoperators en

ISP's kunnen dan ook niet zonder de medewerking van software- en toepassingproviders om samen oplossingen en activiteiten te ontwikkelen. Voorbeelden hiervan zijn OpenDNS/PhishTank, inclusief de bijgehorende zwarte lijsten.

5. PRIORITEITEN VOOR REGELGEVERS

De belangrijkste juridische basis om problemen ten aanzien van Digital Confidence het hoofd te bieden, lijkt aanwezig. Wel moeten bestaande regulerende concepten voortdurend opnieuw geïnterpreteerd met inachtneming van nieuwe technieken en manieren van marketing en gebruik. Het grensoverschrijdende karakter van bedreigingen van Digital Confidence maken internationale (juridische) samenwerking des te noodzakelijker, evenals meer bewustwording van de noodzaak tot actie. Overheden en andere autoriteiten moeten geschikte middelen vinden om nadelige gevolgen te verzachten en partnerships met de sector aangaan.

In de politiek en het reguleringsbeleid lijkt een trend waarneembaar om meer nadruk te leggen op meer medewerking van belanghebbenden dan op meer wetgeving – niet alleen in Europa, maar ook in recente acties van de FCC in de Verenigde Staten. Tegelijkertijd moet de proportionaliteit van regulerend optreden voortdurend worden bekeken, vooral ingeval van zeer interventionistische maatregelen (zoals "three strikes" en verplicht filteren), die mogelijk een inbreuk op fundamentele internetvrijheid en consumentenrechten (bijvoorbeeld wat betreft privacy) zijn en gevestigde juridische zekerheden voor spelers in de sector ondermijnen.

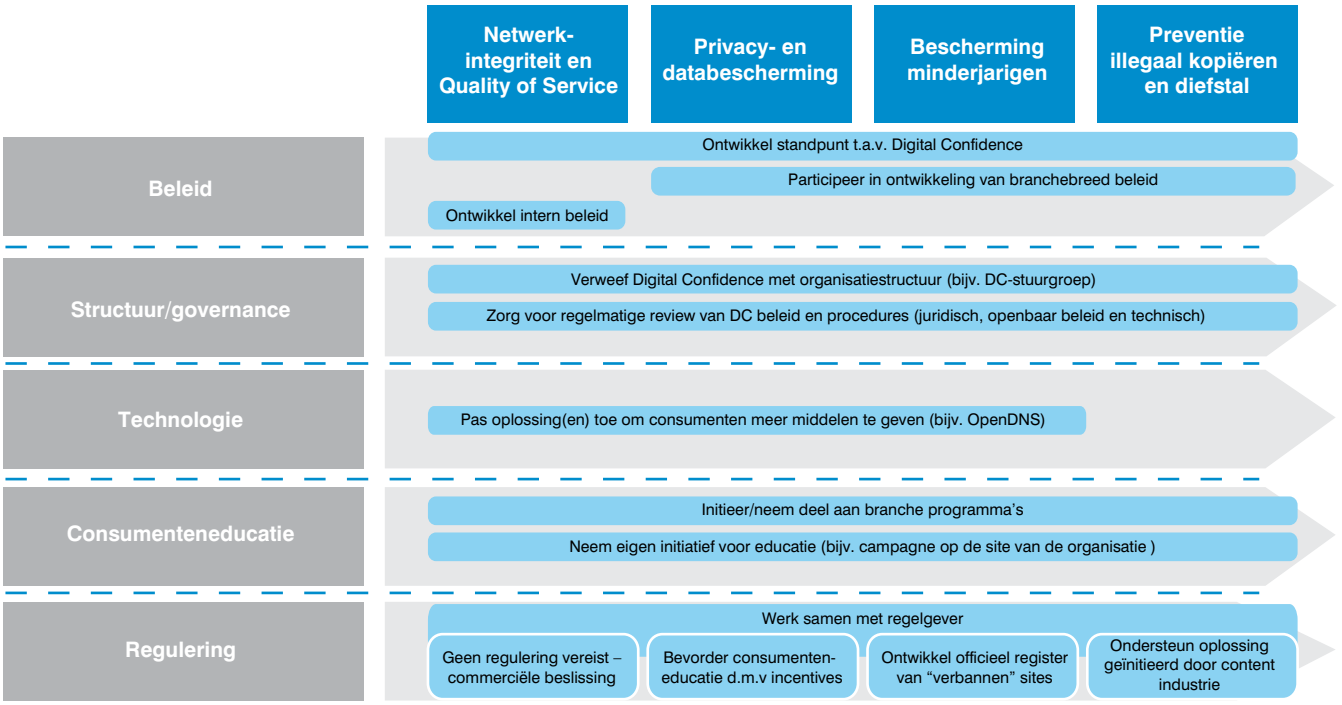
Regelgevers moeten de rol van de netwerkoperator/ ISP begrijpen en de impact van eventuele regulering daarop.

In andere gevallen, zoals het handhaven van zeer strikte vereisten op het gebied van Quality of Service, kan regulerende interventie onvoorziene consequenties hebben voor de bedrijfstak zoals aanzienlijke kosten voor netwerkupgrades. Daarom moeten regelgevers speciaal letten op inter-afhankelijkheid van de verschillende gebieden van Digital Confidence voor de verschillende belanghebbenden en hun besluiten daarop afstemmen.

Ongetwijfeld is er voor regelgevers een belangrijke rol bij het veiligstellen van Digital Confidence. Gezien de grote complexiteit van de kwesties rond Digital Confidence kan de regelgever een belangrijke rol spelen bij het stimuleren van meer samenwerking onder belanghebbenden. Op basis van de analyse in dit rapport zijn dit gebieden die de aandacht van regelgevers zullen belonen:

Regels implementeren zonder rekening te houden met alle mogelijke consequenties, kan leiden tot een grote verliespost voor alle belanghebbenden.

Figuur 62: *Prioriteiten per actiegebied*



Noot: DC = Digital Confidence

• Stimuleer netwerkoperators en ISP's om Digital Confidence-beleid en -procedures vast te stellen, evenals op gedragscodes gebaseerde zelfregulering voor de sector, met name op gebieden waar opdringerige regulerende interventie kan leiden tot negatieve economische resultaten (bijvoorbeeld wat betreft dataverkeermanagement), of fundamentele consumentenrechten kan schenden (bijvoorbeeld de "three strikes"-regel).

• Overweeg maatregelen om het juridische en soms het reputatierisico te beperken voor netwerkoperators en ISP's die Digital Confidencebeleid en -procedures introduceren. Stuur de ontwikkeling bijvoorbeeld aan en stimuleer het sectorbrede gebruik van een register van verbannen sites in het belang van de bescherming van minderjarigen. En breng in Europa eenheid aan in de momenteel per land verschillende benaderingen, onder andere door constructies die het mogelijk maken op internationaal niveau de bescherming van minderjarigen te coördineren.

• Stimuleer de bedrijfstak om een actievere rol te spelen bij het voorlichten van consumenten – zorg voor financiële steun en neem overkoepelende initiatieven tot bredere toepassing, bijvoorbeeld voortbouwend op resultaten van het Safer Internet-programma.

• Zorg voor meer internationale samenwerking om wereldwijde (raamwerken voor) oplossingen te ontwikkelingen voor hoofdzakelijk mondiale problemen, bijvoorbeeld op het gebied van copyrightbescherming.

Samengevat is het laten slagen van Digital Confidence niet noodzakelijkerwijs kostbaar in benodigde investeringen. Aan de andere kant zouden de kosten van mislukking aanzienlijk zijn. Een programma om Digital Confidence te laten slagen is echter niet gemakkelijk en ook niet gratis. De meeste CEO's denken dat hun organisaties al bezig zijn met de bovenomschreven activiteiten – en terecht. Maar in de meeste gevallen zal dat niet genoeg zijn. Digital Confidence reikt verder dan het ter beschikking stellen van informatiemateriaal op de website. Het gaat om op senior niveau samenwerken met vooraanstaande instanties op dit gebied – particulier of publiek – en serieuze campagnes lanceren die daadwerkelijk een verschil maken. Dat vereist financiering en wellicht ook nieuwe vaardigheden binnen de organisaties. Digital Confidence draait niet alleen om het hebben van een beleid voor gegevensbescherming, maar om het creëren van een andere denkwijze binnen een bedrijf, een andere manier van communiceren met klanten en met de maatschappij in het algemeen. Kortom, het succes van Digital Confidence staat of valt met leiderschap vanaf de top.

Het belang van Digital Confidence staat buiten kijf. En er is nog een lange weg te gaan om alle zorgpunten aan te pakken: geen enkel onderdeel van de digitale wereld heeft alle antwoorden of is in staat alle problemen alleen op te lossen. Digital Confidence dient door de sector als geheel aangepakt te worden, met actieve deelneming van de belangrijke belanghebbenden volgens een gemeenschappelijk raamwerk met duidelijke rollen en verantwoordelijkheden. Op deze wijze kan Digital Confidence al haar kracht ontplooien en daarmee voor iedereen in de digitale omgevingen waardescheppende mogelijkheden ondersteunen.

AUTEURS

Thomas Künstner
Vice President
thomas.kuenstner@booz.com
+49 211 3890 143

Michael Fischer
Principal
michael.fischer@booz.com
+49 211 3890 168

John Ward
Senior Associate
john.ward@booz.com
+44 20 7393 3782

Martin F. Brunner
Senior Associate
martin.brunner@booz.com
+49 30 88705 842

Florian Pötscher
Senior Consultant
florian.poetscher@booz.com
+43 1 51822 900

BOOZ & COMPANY WORLDWIDE OFFICES

Asia

Beijing
Hong Kong
Seoul
Shanghai
Taipei
Tokyo

Australia, New Zealand, and Southeast Asia

Adelaide
Auckland
Bangkok
Brisbane
Canberra
Jakarta
Kuala Lumpur
Melbourne
Sydney

Europe

Amsterdam
Berlin
Copenhagen
Dublin
Düsseldorf
Frankfurt
Helsinki
London
Madrid
Milan
Moscow
Munich
Oslo
Paris
Rome
Stockholm
Stuttgart
Vienna
Warsaw
Zurich

Middle East

Abu Dhabi
Beirut
Cairo
Dubai
Riyadh

North America

Atlanta
Chicago
Cleveland
Dallas
Detroit
Florham Park
Houston
Los Angeles
McLean
Mexico City
New York City
Parsippany
San Francisco

South America

Buenos Aires
Rio de Janeiro
Santiago
São Paulo

09/08 Printed in Germany