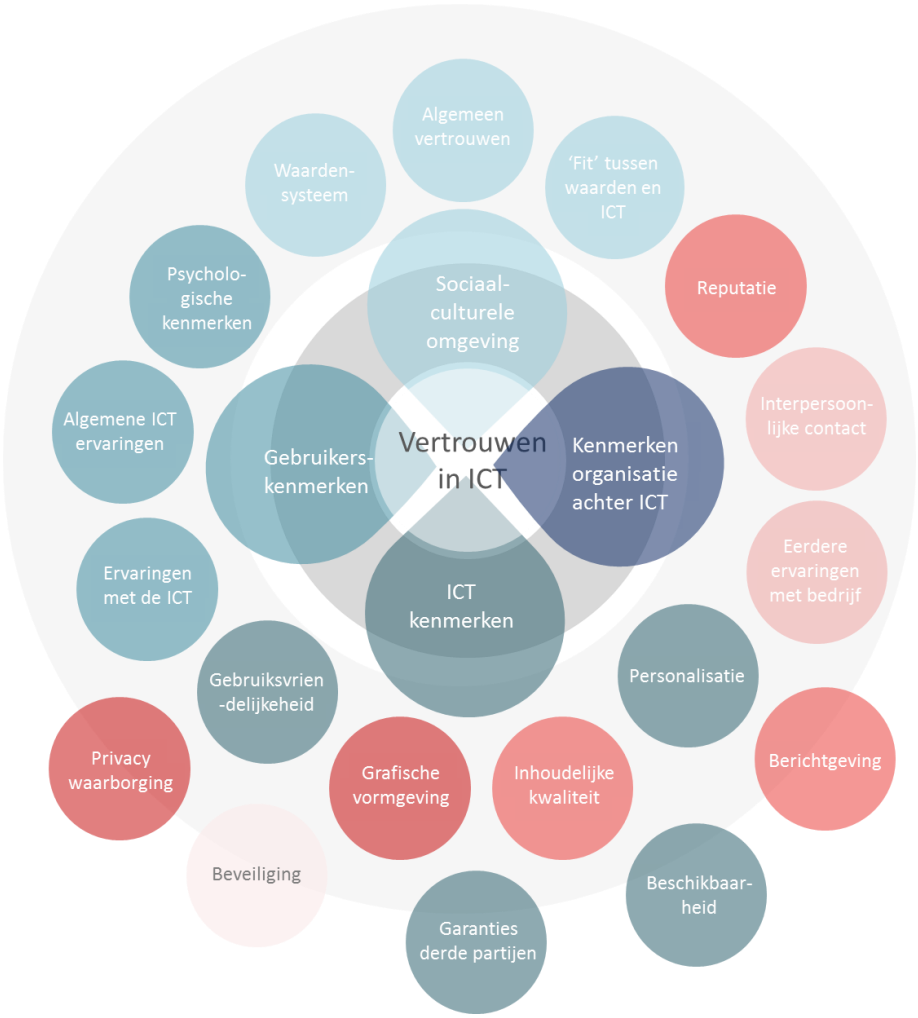
Monitor ICT, veiligheid en vertrouwen

2012



Brassersplein 2
2612 CT Delft
Postbus 5050
2600 GB Delft

www.tno.nl

T +31 88 866 70 00
F +31 88 866 70 57
infodesk@tno.nl

TNO-rapport

Monitor ICT, veiligheid en vertrouwen 2012

Met data over de periode 2011 - 2012

Datum	15 Februari 2013
Auteur(s)	Dr. N.M. (Noor) Huijboom Drs. B.H.A. (Bas) van Schoonhoven (bas.vanschoonhoven@tno.nl)
Aantal pagina's	79
Opdrachtgever	Ministerie van Economische Zaken
Projectnaam	Monitor ICT, veiligheid en vertrouwen 2012
Projectnummer	055.01698/01.04

Samenvatting

Voor het voeren van een overheidsbeleid rond ICT in Nederland wat veiligheid en vertrouwen bevorderd is het nodig dat beleidsmakers een duidelijk beeld hebben van de toestand rond vertrouwen in en veiligheid van ICT. In dit onderzoek hebben we getracht om zowel de veiligheid van ICT in Nederland als het vertrouwen van Nederlanders in ICT in kaart te brengen met zo recent mogelijke data. De monitor is met behulp van subsidie van het ministerie van Economische Zaken tot stand gekomen en wordt gebruikt bij de verdere beleidsontwikkeling.

Sinds de jaren negentig heeft de ontwikkeling en het gebruik van ICT in westerse landen een enorme vlucht genomen. In het dagelijks leven worden vrijwel alle activiteiten – of het nu gaat om bijvoorbeeld werk, zorg of onderwijs – ondersteund door ICT. In 2011 had 94% van de Nederlanders internet toegang thuis en deed 53% online aankopen (Eurostat, 2011). Van de Nederlanders met een betaalrekening had 74% begin 2012 toegang tot internetbankieren (DNB, 2012). Daarnaast hebben steeds meer Nederlanders een smartphone en neemt het mobiele internetgebruik exponentieel toe (OPTA, 2012). Het mag duidelijk zijn dat ICT diep geworteld zijn in de hedendaagse samenleving. Daarmee zijn adequate ICT een belangrijke randvoorwaarde geworden voor innovatie en economische groei. Verschillende studies (zie bijv. Van Ark et al, 2009) tonen aan dat slimme ICT applicaties het produceren, ondernemen en afnemen van diensten efficiënter maken en dat digitale netwerken het ontwikkelen van nieuwe producten en diensten ondersteunen.

Naarmate de afhankelijkheid van ICT toeneemt, wordt ook de veiligheid van en het vertrouwen in ICT belangrijker. Zo kan een uitval van een ICT systeem (bijvoorbeeld door een gerichte aanval) een behoorlijke (organisatorische en financiële) impact hebben en kan suboptimaal gebruik door gebrek aan vertrouwen leiden tot inefficiënties en ineffectiviteit. De feitelijke veiligheid van en het vertrouwen in ICT lijken echter door verschillende factoren te worden bepaald. Natuurlijk zijn ervaringen van gebruikers met onveilige situaties (denk aan misbruik van persoonsgegevens) van fundamentele invloed op het vertrouwen van gebruikers in ICT. Maar uit (o.a. onderhavig) onderzoek blijkt dat wanneer dit soort ervaringen beperkt zijn (bijvoorbeeld tot 5% van de gebruikers), andere factoren een dominante invloed hebben op vertrouwen in ICT. Aspecten die in overwegend veilige situaties belangrijk zijn voor het vertrouwen van een gebruiker zijn bijvoorbeeld grafische vormgeving, gebruiksvriendelijkheid en de mate waarin het bedrijf achter de ICT-dienst een gevestigde partij is.

Met name wat betreft veiligheid was het moeilijk om een adequaat beeld te krijgen. Meldingen van cybercrime worden door burgers en bedrijven vaak niet gedaan, bijvoorbeeld omdat het schadebedrag relatief klein is (in geval van burgers) of vanwege angst voor reputatieschade (in geval van bedrijven). Daarnaast worden meldingen bij betrokken instanties (bijv. politie en justitie) vaak niet naar vorm van cybercrime geregistreerd, maar naar (breder) wetsartikel (bijv. 'diefstal'). Hierdoor is het niet duidelijk bij welke criminele activiteiten ICT een dominante rol hebben gespeeld. Ook worden door verschillende instanties verschillende definities gehanteerd, waardoor cijfers moeilijk te vergelijken zijn. Tot slot worden veel cijfers over cybercrime geleverd door bedrijven die producten en diensten op dit gebied leveren. Deze bedrijven kunnen een prikkel hebben om de grootte van het probleem te overschatten. Alle data gepresenteerd in deze rapportage kunnen slechts begrepen worden als indicaties van ICT (on)veiligheid.

Uit onze enquete komt het volgende beeld ten aanzien van vertrouwen van Nederlanders in ICT naar voren:

- Een klein percentage (5%) van de representatieve steekgroep Nederlanders geeft aan zich "vaak" zorgen te maken over online harassment (zoals agressie, stalken of

pesterij). Daarbovenop geeft 25% aan zich "soms" zorgen te maken over online lastig gevallen worden.

- Respondenten uit de enquete geven aan zich relatief vaak zorgen te maken om besmetting van de computer door een virus (14% vaak, 62% soms), het ontvangen van Spam (27% vaak, 49% soms), of misbruik van hun persoonlijke informatie (21% vaak, 54% soms). Daarnaast is een vaak voorkomende zorg het mogelijk uitvallen van de internetverbinding (16% vaak, 57% soms).
- De zorgen over virussen, Spam en uitval van de internetverbinding lijken samen op te gaan met het relatief vaak ervaren van deze problemen. Dit is bij misbruik van persoonsgegevens niet zo: "slechts" 5% zegt te maken hebben gehad met misbruik van persoonlijke informatie.
- Nederlanders lijken, afgaande op de steekproef, een relatief hoog vertrouwen te hebben in de veiligheid van de ICT infrastructuur (zoals internet, telefonie). Slechts weinigen (minder dan 2%) geeft aan deze diensten (soms) niet te gebruiken wegens gebrek aan vertrouwen in de veiligheid ervan.
- Andere diensten die door een kleine groep Nederlanders minder gebruikt worden omdat de veiligheid niet vertrouwd wordt zijn sociale netwerksites (6%), online winkelen (6%) en internetbankieren (6%). Over het algemeen lijken zorgen om de veiligheid van ICT het gebruiken van die ICT maar weinig in de weg te staan.
- Van de personen die afzien van het gebruik van een dienst wegens onvoldoende vertrouwen in de veiligheid geeft de grootste groep (35%) als reden zorgen om privacy. Daarnaast worden een onbetrouwbaar uiterlijk van een website (23%) en slecht in het nieuws geweest zijn (19%) als redenen genoemd.
- Als het om de *aanbieders* van ICT diensten gaat, geven de respondenten aan vooral de te vertrouwen dat aanbieders van ICT infrastructuur (de "enablers" zoals internet en telefonie toegang) hun veiligheid belangrijk vinden en beschermen (tussen 58% en 63%) en de banken als aanbieders van internetbankieren (62%). Bij het kopen van produkten of diensten online geeft slechts 38% aan dit vertrouwen te hebben.

Uit ons onderzoek komt het volgende beeld ten aanzien van veiligheid van in ICT in Nederland naar voren:

- Het OM registreert de instroom en afdoening van criminaliteit, waaronder enkele specifieke vormen van computercriminaliteit, namelijk: computervredebreuk, aftappen/opnemen, beschadigingen/storen geautomatiseerd werk en onbruikbaar maken van gegevens. In 2011 stroomden 188 zaken op dit vlak in, waarvan het grootste deel (128) computervredebreuk (inbreken in geautomatiseerd werk) betrof.
- Het NCSC handelde in het tweede kwartaal van 2011 tot en met het eerste kwartaal van 2012 in totaal 135 cybercrime incidenten binnen overheden af. Malware infecties kwamen het meest voor (42%), gevolgd door datalekken (12,5%) en phishing (8,8%).
- De Fraudehelpdesk ontving in 2011 van 5.390 personen een melding over een voorval van fraude, waarvan 38% cybercrime (gedefinieerd als fraude middels Internet) en 11% webwinkefraude (valt in registratie Fraudehelpdesk niet onder cybercrime). Hoewel het aantal meldingen van cybercrime het hoogst is, is het aantal gedupeerden het hoogste onder webwinkelfraude. Dit kan verklaard worden doordat cybercrimevormen (zoals phishing) gemeld worden zonder dat de melder gedupeerd is (door tijdige herkenning en/of door schadeloosstelling). De schade per gedupeerde van webwinkelfraude is beperkt omdat het om kleine bedragen gaat voor relatief veel gedupeerden.
- Beveiligingsbedrijf Norton meldt in haar 'Cybercrime Report 2011' dat zij inschat dat in 2011 2,4 miljoen Nederlanders slachtoffer waren van enige vorm van cybercriminaliteit (waaronder ook Spam). Norton raamt de kosten voor Nederlandse slachtoffers in 2011 op 411,9 miljoen euro (direct en indirect financieel verlies). Volgens Norton had in 2011 18% van de Nederlanders te maken met computervirussen

en malware, 2,9% met phishing, 2,1% met hacken van sociale netwerken en 0,43% met online scams.

- CBS laat zien dat (al jaren lang) vermogensmisdrijven de grootste categorie geregistreerde criminaliteit is (in 2010 59% van alle delicten). Binnen de categorie vermogensmisdrijven blijken diefstal, verduistering en inbraak het meest voor te komen (94% van de vermogensdelicten). In welk deel van de zaken ICT een dominante rol speelt (bijv. diefstal gegevens door hacken) is niet bekend.

De cijfers overziend lijkt het aantal Nederlandse burgers dat te maken krijgt met lichtere vormen van cybercrime (bijv. Spam) relatief hoog is, maar dat het aantal dat te maken krijgt met ernstigere vormen (bijv. phishing) vergelijkbaar is met het percentage Nederlanders dat slachtoffer is van 'off-line' criminaliteit. Ook lijken de cijfers erop te wijzen dat de financiele schade die burgers hebben naar aanleiding van 'off line' criminaliteit (bijv. diefstal zonder gebruikmaking ICT, inbraak, misleiding, zakkenrollen) groter is dan de financiele schade die zij lijden aan vormen van cybercrime. Hierbij is het belangrijk om te blijven vermelden dat dit een vertekend beeld kan zijn omdat, niet alle computercriminaliteiten door burgers gemeld worden. Daarnaast worden slachtoffers (bijv. van phishing) veelal schadeloos gesteld, waardoor zij minder schade lijden aan vormen van cybercrime.

In het bedrijfsleven lijken vooralsnog de grotere bedrijven werkzaam in de financiële sector substantiële schade aan vormen van cybercrime (bijv. phishing, skimming en hacken) te ondervinden. Ook de film- en muziekindustrie lijken proportioneel meer getroffen te worden dan andere industrieën (door illegaal downloaden). Hoewel grotere bedrijven over het algemeen beter beveiligde systemen hebben, zit hier meer vermogen en (waardevolle) gegevens en zijn zij daarmee een aantrekkelijk doelwit. De ICT Barometer over Cybercrime van Ernst & Young laat eenzelfde beeld zien. Terwijl van de grote ondernemingen (500+ werknemers) 49% in 2011 schade ondervond door vormen van cybercrime (door Ernst & Young breed geïnterpreteerd, hieronder valt ook Spam) was dat bij kleinere bedrijven (1-19 werknemers) 24%. MKB lijkt vooralsnog vooral last te hebben van traditionele vormen van criminaliteit (diefstal zonder gebruik ICT, inbraak en vernieling). Ook hier geldt weer dat het beeld vertekend kan zijn door beperkte (kwaliteit van de) data.

Vrijwel alle voor dit onderzoek geraadpleegde registraties laten eenzelfde trend over de afgelopen jaren zien; namelijk een toename van cybercrime incidenten. Omdat ICT steeds meer vervlochten is in het dagelijks leven, is het waarschijnlijk dat cybercrime een steeds grotere deel gaat uitmaken van de totale criminaliteit. Met name nieuwe technologieën kunnen hierbij kwetsbaar zijn, omdat deze in het beginstadium vaak nog niet optimaal beveiligd zijn en/of tactieken van criminelen bij gebruikers nog niet bekend zijn. Zo is een waarschijnlijk doelwit de komende jaren mobiele technologie. De beveiliging van de Apps is bijvoorbeeld in gevallen nog onvoldoende en gebruikers zijn beperkt op de hoogte van mogelijke risico's. Daarnaast roepen nieuwe concepten als de 'Cloud' allerlei veiligheidsvraagstukken op. Een voorbeeld betreft de privacy van gebruikers. Omdat de privacywetgeving geldt van het land waarin de gegevens fysiek op een server staan, is het de vraag of de privacy van Nederlanders bij 'Clouds' altijd even goed beschermd is.

Tot slot geeft onderstaande tabel op basis van verschillende rapportages een samenvatting van de percentages Nederlandse individuen en bedrijven die in de periode 2011 – 2012 te maken hadden met specifieke vormen van cybercrime.

Vorm cybercrime	**% Nederlanders**[1]	**% Nederlandse bedrijven**
Website spoofing	4%	10% (Ernst & Young Barometer)
Illegale of aanstootgevende content	8%	6% (EY)
Online harassment	4%	Geen cijfers beschikbaar
Spam	63%	49% (EY)
Phishing	4%	10,3% (EY)
Identiteitsdiefstal	2%	Geen cijfers beschikbaar
Privacy schending	5%	5% diefstal van geg. via computer (EY)
Malware	18%	33% (EY)
Digitale spionage	NVT	10 door AIVD onderkende incidenten
DDoS attacks	NVT	4% (EY)
Website defacement	NVT	3%
Storingen	21%	

Tabel 1, Overzicht percentages Nederlandse individuen en bedrijven die in 2011 en begin 2012 te maken hadden met vormen van cybercrime, Bron: TNO, Ernst & Young, Norton en AIVD

[1] De cijfers over Nederlandse burgers zijn afkomstig uit de TNO enquête in het kader van dit onderzoek. Hierin was “Phishing” en ”Website spoofing” in één vraag samen genomen: dit percentage is door tweeën gedeeld en dus mogelijk niet accuraat.

Figuren en tabellen

Tabellen

Tabel 1, Overzicht percentages Nederlandse individuen en bedrijven die in 2011 en begin 2012 te maken hadden met vormen van cybercrime, Bron: TNO, Ernst & Young, Norton en AIVD 6
Tabel 2, Computer vaardigheden van individuen in 2011, Bron: Eurostat. 33
Tabel 3, Frequentie identiteitsfraude van een grootbank in 2010 en eerste twee maanden van 2011, Bron: PWC 47
Tabel 4, Door NCSC afgehandelde incidenten met uitgelekte gegevens, Bron: NCSC 51
Tabel 5, Aantallen meldingen voorvallen privacy schending 2011, Bron: CBP 51
Tabel 6, Type melding per hoofdsector 2011, Bron: CBP 52
Tabel 7, percentage van ondervraagden dat in aanraking kwam met specifiek type cybercrime tussen april 2010 en maart 2011, Bron: Norton 73

Figuren en grafieken

Figuur 1, Vertrouwen in ICT: perceptie en cyber-indicatoren, TNO 2010 12
Figuur 2, Vertrouwen in en veiligheid van ICT; perceptiefactoren voor vertrouwen en veiligheidsindicatoren, TNO 2012 13
Figuur 3, Typologie van factoren die van invloed zijn op het vertrouwen van gebruiker in een ICT, TNO 2012 15
Figuur 4, Overzicht van factoren die van invloed zijn op het vertrouwen van gebruiker in ICT, TNO 2012 18
Figuur 5, Factoren (en indicatoren) die de veiligheid van ICT bepalen, TNO 2012 20
Figuur 6 - “Hoe vaak heeft u de afgelopen 6 maanden van onderstaande diensten gebruik gemaakt?” 22
Figuur 7, vertrouwen in zeven instituties, bevolking van 18+, 2008-2012 (in procenten), Bron: SCP, COB 2008/1-2012/1 25
Figuur 8, percentage vertrouwen in nationale instituties (defensie, rechtspraak, nationale overheid) 2010, Bron: OECD, Society at a Glance, 2011 26
Figuur 9, vertrouwenstypen, bevolking van 18+, 2011-2012 (in procenten), Bron: SCP, COB 2012/1 26
Figuur 10, opvattingen over samenleving, bevolking van 18+, 2008 (in procenten), Bron: SCP, COB 2008/1-2012/1 27
Figuur 11, vertrouwen in anderen, 2004 (in procenten), Bron: European Social Survey 27
Figuur 12, Percentage Nederlanders dat vertrouwen heeft in anderen, periode 1981-2012, gebaseerd op cijfers van Wold Value Survey, European Social Survey en COB van SCP 28
Figuur 13, Percentage burgers dat in 2008 een groot vertrouwen in anderen had, Bron: OECD Society at a Glance 2011, ... 28
Figuur 14, Percentage burgers dat in 2008 een groot vertrouwen in anderen had, Bron: European Social Survey, ... 29
Figuur 15, “Heeft u in de afgelopen 6 maanden een van de onderstaande diensten niet gebruikt omdat u de veiligheid van de dienst niet vertrouwde?” 30
Figuur 16, “Hebben zorgen over veiligheid u doen afzien van de volgende activiteiten in de afgelopen 6 maanden?” 31
Figuur 17, “Heeft u in de afgelopen 6 maanden een van de onderstaande diensten niet gebruikt omdat u de veiligheid van de dienst niet vertrouwde?” 31
Figuur 18, “Hebben zorgen over veiligheid u doen afzien van de volgende activiteiten in de afgelopen 6 maanden?” 32
Figuur 19, Gebruikmaking zoekmachine door individuen 2005-2011, Bron: Eurostat. 33

Figuur 20, Telefoneren via het Internet door Nederlanders 2005-2011, Bron: CBS. 34
Figuur 21, Percentage individuen dat in toekomst meer nadruk op technologie wil, Bron: World Values Survey. 34
Figuur 22, Percentage internet gebruikers dat online goederen of diensten bestelden, 2009-2011, Bron: Eurostat. 35
Figuur 23, 2011, Percentage individuen dat ICT niet gebruikt om specifieke reden, Bron: CBS. 36
Figuur 24, “Hoe vaak maakt u zich zorgen over de volgende mogelijke problemen rond privé-internetgebruik?” 37
Figuur 25, “Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?“ 38
Figuur 26, “Hebben zorgen over veiligheid u doen afzien van de volgende activiteiten in de afgelopen 6 maanden?” 38
Figuur 27, “Heeft u in de afgelopen 6 maanden een van de onderstaande diensten niet gebruikt omdat u de veiligheid van de dienst niet vertrouwde?” 39
Figuur 28, “Waarom vertrouwde u deze dienst(en) niet?” 39
Figuur 29, “Hoeveel vertrouwen heeft u dat aanbieders van de volgende ICT diensten uw veiligheid belangrijk vinden en beschermen?” 41
Figuur 30, Gemeten Spam volume 2005 tot en met 2011, Bron: Symantec 43
Figuur 31, Gemeten Spam volume 2010-2011, Bron: M86 Security 43
Figuur 32, Percentage respondenten dat aangeeft in 2011 last te hebben gehad van o.a. Spam, Bron: Ernst & Young 44
Figuur 33, “Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?” 44
Figuur 34, “Welke software gebruikt u om uw computer te beschermen?” 44
Figuur 35, Gemeten phishing rate 2005 tot en met 2011, Bron: Symantec 45
Figuur 36, Raming schade door o.a. fraude met Internetbankieren 2010 en 2011 Bron: DNB 46
Figuur 37, Percentage respondenten dat in 2011 te maken heeft gehad met verschillende vormen van phishing, Bron: Ernst & Young 47
Figuur 38, “Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?” 48
Figuur 39, Landen waarin ten minste 1 voorval van data breach is gevonden, Bron: Verizon 49
Figuur 40, Percentage data breaches per agent, Bron: Verizon 49
Figuur 41, Percentage agents per motief om tot data breach over te gaan, Bron: Verizon 50
Figuur 42, Aantallen gelekte records in de jaren 2004-2011, Bron: Verizon 50
Figuur 43, Percentage respondenten dat aangeeft in 2011 last gehad te hebben van o.a. diefstal van gegevens, Bron: Ernst & Young 51
Figuur 44, Percentage respondenten per vraag over consent, Bron: Enisa 53
Figuur 45, Percentage respondenten dat user tracking mechanismen gebruikt, Bron: Enisa 53
Figuur 46, Percentage respondenten dat persoonlijke data verzamelt voor het leveren van diensten en voor commercieel gebruik, Bron: Enisa 54
Figuur 47, Percentage respondenten dat persoonlijke data deelt met specifieke partijen, Bron: Enisa 54
Figuur 48, Percentage ondervraagden dat in aanraking kwam met onaardig of gemeen gedrag op social networking sites, Bron: PEW Research Center 55
Figuur 49, Percentage ondervraagden dat in 2011 was gepest via verschillende media, Bron: PEW Research Center 55
Figuur 50, “Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?” 56

Figuur 51, Unieke phishing sites gedetecteerd tussen januari en december 2011, Bron: APWG 58
Figuur 52, Percentage respondenten dat meldt last te hebben gehad van phishing activiteiten in 2011, Bron: Ernst & Young 58
Figuur 53, Percentage respondenten dat te maken heeft gehad met identiteitsdiefstal in jaren 2007-2011 (2011 januari en februari), Bron: PWC 59
Figuur 54, Percentage respondenten dat aangeeft te maken te hebben gehad met een specifieke vorm van identiteitsfraude, Bron: PWC 60
Figuur 55, “Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?” 60
Figuur 56, Inschatting illegale content wereldwijd 2011 – pornografie als niet illegaal begrepen, Bron: Envisional 61
Figuur 57, Percentage respondenten dat meldt last te hebben gehad van o.a. verspreiden van illegaal materiaal via computersystemen van organisatie in 2011, Bron: Ernst & Young 62
Figuur 58, “Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?” 62
Figuur 59, Virus rate gemeten in verschillende landen in jaren 2005 tot en met 2011, Bron: Symantec 63
Figuur 60, Nieuwe malware sites per dag over de jaren 2001 tot en met 2011, Bron: Symantec 63
Figuur 61, Malware functionaliteit per percentage datalek door malware, Bron: Symantec 64
Figuur 62, Percentage malware per type over periode juli 2010 tot en met juni 2012, Bron: Surfright/NCSC 65
Figuur 63, Infectiegraad Nederlandse PC’s over periode juli 2010 tot en met juni 2012, Bron: Surfright/NCSC 65
Figuur 64, Percentage respondenten dat in 2011 last had van o.a. malware, Bron: Ernst & Young 65
Figuur 65, Percentage respondenten dat in 2011 last heeft gehad van o.a. het door hackers bekladden van de homepage van hun organisatie, Bron: Ernt & Young 66
Figuur 66, “Hoe lang heeft u van de onderstaande diensten geen gebruik kunnen maken door een technische storing in de afgelopen 6 maanden?” 67
Figuur 67, Percentage incidenten per dienst. Bron: ENISA, 2012 68
Figuur 68, Percentage incidenten per oorzaak. Bron: ENISA, 2012 68
Figuur 69, Gemiddelde duur incident per oorzaak in uren. Bron: ENISA, 2012 68
Figuur 70, “Heeft u de afgelopen 6 maanden schade opgelopen door problemen bij internet gebruik?” 69
Figuur 71, Gemiddeld aantal trageted attacks tegengehouden door Symantec.cloud per dag wereldwijd in 2011, Bron: Symantec 70
Figuur 72, Totale schade geleden door gedupeerden per fraudetype, Bron: Fraudehelpdesk 71
Figuur 73, Gemiddelde schade per gedupeerde per fraudetype, Bron: Fraudehelpdesk 72
Figuur 74, Maatschappelijke schade op jaarbasis, in mln euro, prijzen 2009, Bron: WODC 73

Inhoudsopgave

1 Inleiding 11
1.1 Beleidskader veiligheid en vertrouwen in ICT 11
1.2 Informatie- en Communicatie Technologie (ICT) 11
1.3 Monitoren van veiligheid van en vertrouwen in ICT 12
1.4 Doel van de publicatie 13
1.5 Opzet publicatie 13

2 Concepten vertrouwen en veiligheid 15
2.1 Het begrip 'Vertrouwen in ICT' 15
2.2 Factoren die het vertrouwen in ICT beïnvloeden 15
2.3 Het begrip 'Veiligheid van ICT' 18
2.4 Factoren die veiligheid van ICT bepalen 19

3 Methodologie 21
3.1 Onderdeel vertrouwen in ICT 21
3.2 Onderdeel veiligheid van ICT 22

4 Vertrouwen in ICT 24
4.1 Sociaal-culturele omgeving 24
4.2 Gebruikerskenmerken 30
4.3 ICT kenmerken 37
4.4 Kenmerken organisatie achter ICT 41

5 Veiligheid van ICT 42
5.1 Exclusiviteit 42
5.2 Integriteit 57
5.3 Beschikbaarheid 67
5.4 Algemene cijfers cybercrime 71

6 Conclusie 74

7 Literatuur, documenten en websites 76

1 Inleiding

1.1 Beleidskader veiligheid en vertrouwen in ICT

In mei 2011 lanceerde het Ministerie van Economische Zaken de 'Digitale Agenda.nl, ICT voor innovatie en economische groei', waarin het ICT beleid voor de periode van 2010-2015 wordt geschetst. Het centrale uitgangspunt van de agenda is dat adequate ICT een belangrijke voorwaarde is voor *innovatie en economische groei in Nederland*. Om kansen van ICT optimaal te benutten, zijn in de agenda vier actielijnen geformuleerd; (1) het stimuleren van slimmer ondernemen met behulp van ICT, (2) het bevorderen van een snelle en open infrastructuur, (3) het versterken van vertrouwen in ICT en waarborgen van digitale veiligheid, en (4) het vergroten van e-vaardigheden en het onderhouden van een goede ICT onderzoeksinfrastructuur.

Voorliggende monitor gaat met name in op actiepunt 3 van de agenda. De monitor is dankzij subsidie van het ministerie van Economische Zaken tot stand gekomen en wordt gebruikt bij de verdere beleidsontwikkeling.

ICT is een belangrijke randvoorwaarde voor innovatie en economische groei. Zo stimuleren digitale (sociale) netwerken bijvoorbeeld 'bottom-up' innovatie en maken slimme applicaties het produceren, ondernemen en afnemen van diensten efficiënter (zie bijv. Van Ark et al, 2009). Het mag duidelijk zijn dat Nederland alleen dan internationaal kan concurreren, wanneer adequate ICT optimaal worden gebruikt. Van belang is dan ook om de juiste randvoorwaarden te creëren voor een goede ontwikkeling en gebruik van ICT. Als het gaat om een *optimaal ICT gebruik*, zijn factoren als *vertrouwen in en veiligheid van ICT cruciaal*. ICT wordt door gebruikers meest intensief toegepast wanneer de gepercipieerde baten opwegen tegen de kosten en risico's van het gebruik. Wanneer het gebruik van een ICT-dienst bijvoorbeeld tijdwinst oplevert, de kosten relatief laag zijn en de kans klein is dat de gebruiker's belangen worden geschaad zal de drempel laag zijn om de betreffende ICT-dienst te gebruiken.

In de Digitale Agenda.nl benadrukt het Ministerie van Economische Zaken dat uitval en misbruik van ICT kan leiden tot een afnemend vertrouwen en daarmee een rem kan zijn op ICT gebruik. De agenda bouwt voort op de 'Nationale Cyber Security Strategie' (2010), welke een werkplan omvat voor veilige en betrouwbare ICT[2]. Waar de Nationale Cyber Security Strategie voornamelijk hoofdlijnen schetst voor een effectief veiligheidsbeleid (bijv. aanwezigheid van een Cyber Security Raad), wordt de Digitale Agenda concreter. Belangrijke *actielijnen* in de agenda zijn bijvoorbeeld: (a) de aanpak van botnets, (b) het vergroten van de beschikbaarheid van netwerken, (c) het bevorderen van veilige ICT producten, (d) het waarborgen van privacy en (e) het versterken van veilig online zaken doen. In de Digitale Implementatie Agenda.nl zijn deze actielijnen uitgewerkt in twee hoofddoelen (met bijbehorende acties): (1) het waarborgen van continuïteit van de ICT infrastructuur en (2) het stimuleren van kennis over veilig gebruik van ICT[3].

1.2 Informatie- en Communicatie Technologie (ICT)

In deze monitor draait alles om de veiligheid van ICT en het vertrouwen daarin. De afkorting ICT staat daarbij voor *Informatie- en Communicatie Technologie*, en is een brede

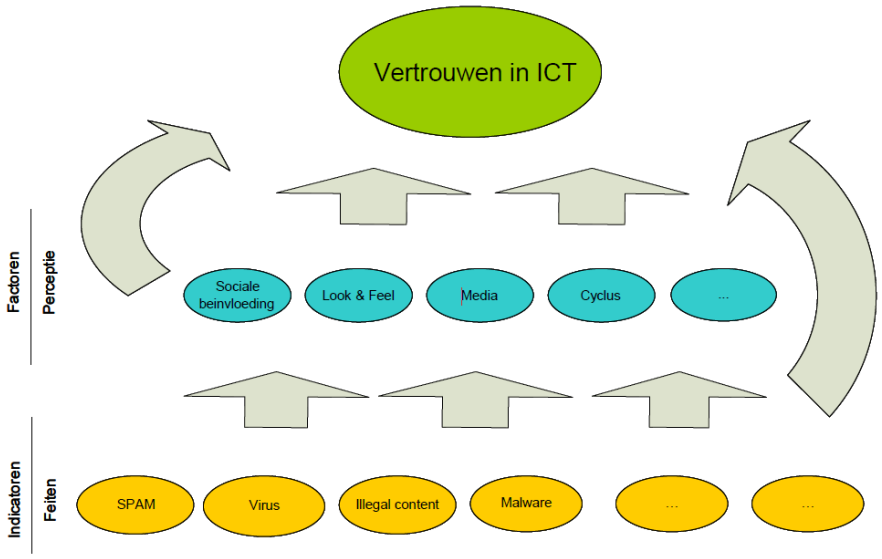
[2] Onderdeel van deze strategie zijn onder andere: (a) het inrichten van een Cyber Security Raad en National Cyber Security Centrum, (b) het opstellen van dreiging- en risicoanalyses, (c) het vergroten van de weerbaarheid van vitale infrastructuren, (d) het ontwikkelen van responscapaciteit om ICT-verstoringen te pareren, (e) het intensiveren van opsporing en vervolging van cybercrime en (f) het stimuleren van onderzoek en onderwijs.

[3] Zie ook Programma DigiVeilig – ondergebracht bij ECP.

verzamelterm waaronder computer- en communicatieapparatuur en software applicaties die gebruikt worden om informatie te verzamelen, communiceren, verwerken en op te slaan. ICT betreft bijvoorbeeld websites, mobiele telefoons, tekstverwerkingspplicaties of de internetinfrastructuur. In deze monitor wordt het begrip ICT gebruikt om in algemene zin over alle zaken te spreken die onder ICT geschaard worden

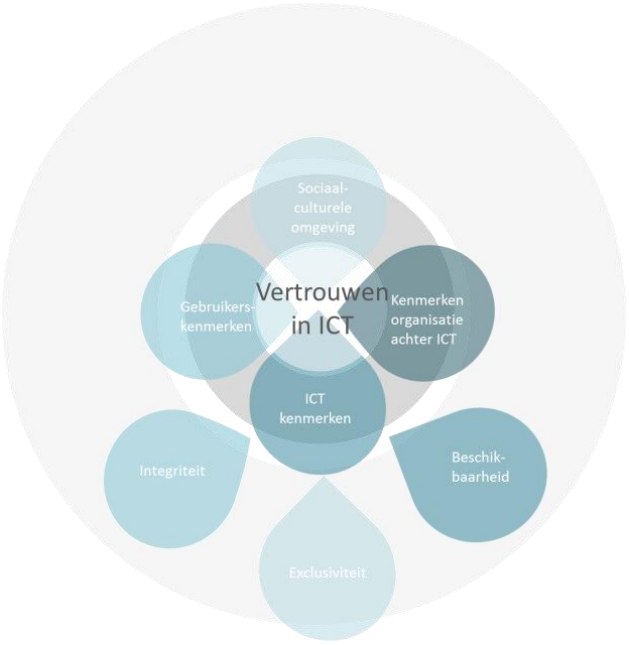
1.3 Monitoren van veiligheid van en vertrouwen in ICT

In 2010 heeft TNO een notitie geschreven voor het *monitoren van veiligheid en vertrouwen van ICT*. Om progressie naar aanleiding van de ondernomen actiepunten van de Digitale Agenda in kaart te brengen en toekomstig beleid vorm te geven is het van belang om te monitoren. Zo kan op basis van gemeten indicatoren beleid worden bijgesteld en prioriteit worden gegeven aan specifieke aspecten van het gevoerde beleid. In de notitie van TNO is onderstaand model (figuur 1) gepresenteerd om te komen tot een overzicht van relevante variabelen voor het monitoren van veiligheid en vertrouwen in ICT. In het model wordt de relatie gelegd tussen de perceptiefactoren die vertrouwen in ICT beïnvloeden (zie middelste laag figuur 1) en de feitelijke cyber-indicatoren (zie onderste laag figuur 1). De 'look and feel' van een ICT applicatie kan bijvoorbeeld het idee van een gebruiker dat een ICT veilig is beïnvloeden en de mate van aanwezigheid van illegale content zegt iets over de feitelijke veiligheid van een ICT. Het model maakt expliciet onderscheid tussen gebruikersperceptie en feitelijke veiligheid omdat hier een discrepantie tussen kan zijn; gebruikers kunnen vertrouwen hebben in onveilige ICT of een veilige ICT wantrouwen.



Figuur 1, Vertrouwen in ICT: perceptie en cyber-indicatoren, TNO 2010

Om tot een gedegen monitor te komen, zijn in dit project zowel de perceptiefactoren als de feitelijke indicatoren van het model verder uitgewerkt. Voor het in kaart brengen van perceptiefactoren is een uitgebreide literatuurstudie uitgevoerd en voor het identificeren van feitelijke indicatoren is data-onderzoek verricht. Beide onderzoeksmethoden hebben geleid tot een overzicht van factoren en indicatoren welke zijn geclusterd naar '*type' factor en indicator* en weergegeven in onderstaand model (figuur 2). De factoren en indicatoren zoals genoemd in figuur 1 vallen onder specifieke *typen* van factoren en indicatoren (zo valt 'look and feel' bijvoorbeeld onder het type factoren 'kenmerken van de ICT' en is aanwezigheid van 'illegale content' een indicator voor mate van 'integriteit').



Figuur 2, Vertrouwen in en veiligheid van ICT; perceptiefactoren voor vertrouwen en veiligheidsindicatoren, TNO 2012

Vertrouwen van gebruikers in ICT (zie kern van figuur 2) wordt bepaald door vier typen factoren (zie binnenste ring figuur 2), namelijk: de *sociaal-culturele omgeving* van gebruikers (denk aan culturele kenmerken zoals mate van risicomijding), *gebruikerskenmerken* (bijvoorbeeld de mate waarin gebruikers ervaren zijn in ICT gebruik), *ICT kenmerken* (denk aan beschikbaarheid van ICT, maar ook grafische vormgeving en inhoudelijk kwaliteit) en de *organisaties achter de ICT* (bijvoorbeeld de reputatie van organisaties). De feitelijke veiligheid van ICT (zie buitenste ring figuur 2) is gerelateerd aan de *ICT kenmerken* (de mate van aanwezigheid van illegale content vormt bijvoorbeeld input voor de kwaliteit van de content van de ICT). De indicatoren voor de feitelijke veiligheid kunnen worden onderverdeeld in drie typen (overgenomen van het Ministerie van EZ, 2010), namelijk: (a) *integriteit* (aanwezig zijn van correcte en volledige informatie en software), (b) *exclusiviteit* (mate van bescherming van gevoelige informatie tegen onbevoegd en ongeautoriseerd gebruik) en (c) *beschikbaarheid* (van applicaties, informatie en diensten voor gebruikers). Het model wordt verder geoperationaliseerd in hoofdstuk 2. Dit model is als basis gebruikt voor de monitor en zal komende jaren verder verder verfijnd worden op basis van de resultaten van de monitor.

1.4 Doel van de publicatie

Het doel van deze publicatie is tweeledig. Ten eerste beoogt het inzicht te verschaffen in factoren die het vertrouwen van gebruikers in ICT beïnvloeden en indicatoren te identificeren om de feitelijke veiligheid van ICT te meten. In de tweede plaats tracht de publicatie een beeld te geven van het vertrouwen van Nederlanders in ICT en de veiligheid van ICT. Zoals eerder gesteld is het zeer moeilijk gebleken om betrouwbare data te vinden over de feitelijke veiligheid van ICT; de gepresenteerde data in dit rapport geven een indicatie van veiligheid van ICT.

1.5 Opzet publicatie

In hoofdstuk 1 van de rapportage is het beleidskader omtrent veiligheid en vertrouwen in ICT geschetst. Hoofdstuk 2 verkent de concepten ‘vertrouwen’ en ‘veiligheid’ en presenteert een model van indicatoren om vertrouwen en veiligheid te kunnen monitoren.

Hoofdstuk 3 beschrijft de toegepaste methodologie om te komen tot de resultaten van dit onderzoek. De specifieke data gevonden ten aanzien van de mate waarin Nederlanders vertrouwen hebben in ICT en de veiligheid van Nederlandse ICT worden uiteengezet in respectivelijk hoofdstukken 4 en 5. Een confrontatie van 'vertrouwen in ICT' en 'veiligheid van ICT' vindt plaats in hoofdstuk 6.

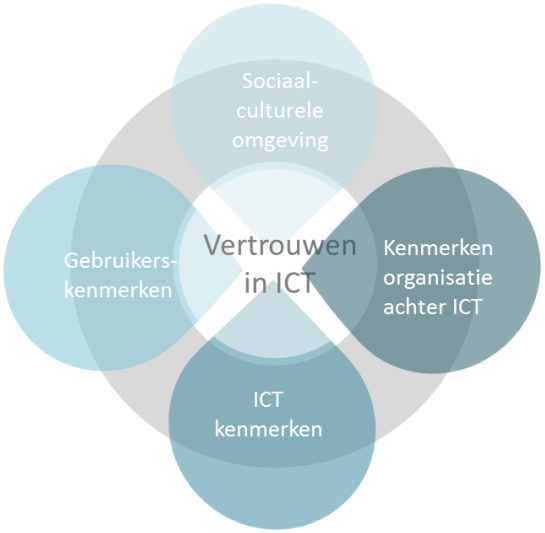
2 Concepten vertrouwen en veiligheid

2.1 Het begrip 'Vertrouwen in ICT'

Hoewel wetenschappers het erover eens zijn dat vertrouwen een belangrijke voorwaarde is voor het gebruik en de acceptatie van ICT, bestaat er geen eenduidig begrip van het concept 'vertrouwen'. Terwijl sommigen de nadruk leggen op vertrouwen als een *perceptie* van risico's (bijv. Lane & Bachmann, 1998; Rousseau et al., 1998), zien anderen de *acceptatie* van risico's als belangrijkste element van vertrouwen (bijv. Doney, Cannon, & Mullen, 1998). Corritore et al. (2003) bieden een handzame definitie van vertrouwen in relatie tot ICT, namelijk: "*Online trust is an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited*". Met andere woorden: vertrouwen in ICT kan worden begrepen als een verwachting van een gebruiker dat zijn/haar belangen niet worden geschaad tijdens het gebruik van de ICT.

2.2 Factoren die het vertrouwen in ICT beïnvloeden

Vertrouwen van gebruikers in ICT wordt bepaald door een aanzienlijke set van factoren (Beldad, 2011). Het verschil tussen vertrouwen in een persoon en in een ICT is dat vertrouwen in een ICT meer lagen kent (Shankar et al., 2002). De gebruiker heeft niet alleen verwachtingen ten aanzien van de *ICT* zelf (bijv. beschikbaarheid en beveiliging) maar ook de *organisatie* achter de ICT (bijv. competentie, welwillendheid en integriteit van de organisatie). Net als bij 'offline' trust wordt 'online' trust daarnaast bepaald door de *sociaal culturele omgeving* van de gebruiker (bijv. algemeen gevoel van vertrouwen) en *kenmerken van de gebruiker* (bijv. individueel psychologische kenmerken en ervaringen). Figuur 3 geeft de typologie van factoren die van invloed zijn op het vertrouwen van een gebruiker in een ICT beknopt weer. Deze zullen in de volgende paragrafen worden uitgewerkt.



Figuur 3, Typologie van factoren die van invloed zijn op het vertrouwen van gebruiker in een ICT, TNO 2012

2.2.1 Sociaal culturele omgeving van de gebruiker

Hoewel het aantal studies over de effecten van sociaal-culturele factoren op het vertrouwen van gebruikers in ICT beperkt is, zijn er enkele onderzoeken die verbanden aantonen. Yoon (2009) demonstreerde bijvoorbeeld in zijn onderzoek naar het gebruik en de acceptatie van e-commerce in China dat *culturele waarden* zoals risicomijding een effect

hebben op de mate van vertrouwen in en het gebruik van ICT. Yoon's onderzoek duidt erop dat hoe risicomijdender de cultuur in een land is, hoe lager het vertrouwen en het gebruik van e-commerce diensten. Daarnaast betogen Siala et al. (2003) dat *overeenkomsten* tussen de waarden geuit in de ICT en de waarden van de gebruiker het vertrouwen in een ICT kunnen verhogen. In het onderzoek van Siala et al. hadden Moslims bijvoorbeeld een groter vertrouwen in Moslim websites dan in Christelijke websites. Kirs et al. (2012) leggen een verband tussen het *nationale level van vertrouwen* en de mate van ICT adoptie in een land. De onderzoeksresultaten van Kirs et al. geven een sterke empirische basis voor de relatie tussen 'algemeen vertrouwen' in een land en de generieke adoptie van ICT; hoe hoger het algemeen vertrouwen, hoe hoger het vertrouwen in ICT (en bedrijven achter de ICT) en hoe hoger de ICT adoptie.

2.2.2 Gebruikerskenmerken

Het vertrouwen in een ICT verschilt van persoon tot persoon en kan toenemen en afnemen (in de tijd en afhankelijk van de situatie). Een factor voor het vertrouwen van een persoon in een ICT is dan ook zijn/haar persoonlijke *psychische gesteldheid*. Zoals Mayer et al. (1995) stellen: "Some people are just more trusting than others". Meer specifiek; variaties in persoonlijk vertrouwen kunnen verklaard worden door verschillen in culturele achtergrond, persoonlijkheden, persoonlijke ontwikkeling en ervaringen. Gefen (2000) vond in zijn onderzoek dat er een positief verband bestaat tussen het *algemeen vertrouwen* van een persoon en het vertrouwen dat hij/zij heeft in ICT. Naast psychische kenmerken is veel geschreven over de relatie tussen de *algemene ICT ervaringen* van een gebruiker en het vertrouwen dat hij/zij heeft in specifieke ICT toepassingen. Hoewel lang werd aangenomen dat gebruikers met veel ICT ervaring een hoger vertrouwen hebben in ICT toepassingen, toonden Aiken en Bousch (2006) aan dat wanneer het gaat om expert gebruikers het vertrouwen in specifieke ICT juist weer kan afnemen. Deze expert gebruikers zien (meer dan minder ervaren gebruikers) de tekortkomingen van een ICT, waardoor hun vertrouwen kan afnemen. Tot slot hebben *eerdere ervaringen* van een gebruiker met de specifieke ICT of gelijksoortige ICT invloed op het vertrouwen in de ICT. Lee et al. (2012) demonstreerden in hun recente onderzoek naar het delen van informatie op sociale media websites dat eerder ervaringen met een bepaalde website of gelijksoortige websites het vertrouwen in en gebruik van de website kunnen vergroten.

2.2.3 Kenmerken van de betreffende ICT

Een derde set van factoren die van invloed is op het vertrouwen van een gebruiker in een ICT zijn de kenmerken van de betreffende ICT (zie bijv. Beldad, 2011). Een belangrijke determinant voor vertrouwen in ICT is de gepercipieerde *gebruiksvriendelijkheid* van de ICT. Bart et al. (2005) vonden in hun studie naar vertrouwen in e-commerce websites dat het vertrouwen van gebruikers in gebruiksvriendelijke websites (waarop klanten op een eenvoudige en snelle manier konden vinden wat ze zochten) hoger was dan in minder gebruiksvriendelijke websites. Een hiermee samenhangende factor is de *grafische vormgeving* van de ICT. Kim en Moon (1998) onderzochten de effecten van het gebruik van specifieke grafische toepassingen zoals Clipart en het ontwerp van de user interface (bijvoorbeeld kleur en lay-out) van een website van een bank. Uit het onderzoek bleek dat het gebruik van grafische toepassingen, bepaalde kleuren en mate van symmetrie effect hadden op het vertrouwen van de gebruikers. Liao et al. (2006) vonden dat de *inhoudelijke kwaliteit* van e-commerce websites (bruikbaarheid, accuraatheid en compleetheid van de informatie) een positief effect had op het vertrouwen van de gebruikers. Ook *personalisatie* van de website heeft volgens wetenschappers een effect op het vertrouwen van de gebruiker al is dit effect niet eenduidig. Wanneer de klant beter bediend wordt door personalisatie kan dat het vertrouwen vergroten (Briggs et al, 2004), maar het gebruik van persoonlijke informatie voor personalisatie kan het vertrouwen juist weer verlagen.

Studies naar het verband tussen vertrouwen in een ICT en *privacy waarborging* geven strijdige resultaten. Terwijl de onderzoeksresultaten van sommige studies erop wijzen dat een sterker privacy beleid leidt tot meer vertrouwen (bijv. Lauer & Deng, 2007), geven andere onderzoeken aan dat gebruikers weinig oog hebben voor privacy waarborgen (bijv. Arcand et al. 2007) en dat de waarborgen weinig effect hebben op acceptatie en gebruik van de ICT. Een adequate *beveiliging* van een ICT lijkt echter wel een substantieel effect te hebben op het vertrouwen van een gebruiker in de ICT (Yoon, 2002, O'Reilly & Finnegan, 2005, Bus, 2005). Bus (2005) benadrukte bijvoorbeeld dat een beveiligde infrastructuur, identificatie, authenticatie en digitaal 'asset managagement' cruciaal zijn voor het vertrouwen van gebruikers in ICT. Daarnaast wijzen verschillende studies er op dat *garanties of aanbevelingen van derde (gevestigde) partijen* (denk aan certificeringsinstituten of grote gevestigde bedrijven zoals Ahold) een positief effect kunnen hebben op het vertrouwen van een gebruiker in een ICT (zie bijv. Koehn, 2003). *Beschikbaarheid* – het percentage van de tijd dat de ICT operationeel is – is volgens Lai et al. (2011) een andere factor die het vertrouwen van de gebruiker in de ICT kan beïnvloeden. In sommige studies wordt ook *Spam* genoemd als mogelijk factor die het vertrouwen van een gebruiker negatief beïnvloedt (Hoffman et al., 1999).

Een laatste factor die het vertrouwen van een gebruiker in een ICT bepaalt is *berichtgeving*. Dit kan berichtgeving zijn door traditionele media (bijv. journaal en kranten) maar kan ook bestaan uit Internet reviews en ratings van een ICT (zie bijvoorbeeld Corritore et al., 2003; Sparks et al., 2011). Sparks et al. (2011) onderzochten bijvoorbeeld de effecten van online reviews op het vertrouwen van gebruikers in websites met toeristische producten (bijv. hotelboekingen). Uit hun onderzoek bleek dat het vertrouwen van gebruikers vooral beïnvloed werd door negatieve informatie, met name in de gevallen waarin de gehele set van reviews negatief was. Echter, positieve informatie weergegeven met onder andere numerieke rating leek het vertrouwen van de gebruiker te vergroten (zie ook Jøsang et al., 2007).

2.2.4 Kenmerken organisatie achter de ICT

Een laatste set van factoren betreft de eigenaar van de ICT. Verschillende studies naar het gebruik van e-commerce websites hebben aangetoond dat er een sterk verband bestaat tussen de *reputatie* van het bedrijf dat eigenaar is van de ICT en het vertrouwen van de gebruiker in de ICT (zie bijv. Corritore et al, 2003; Jøsang et al., 2007; Bente et al., 2012). Een andere belangrijke determinant voor vertrouwen is de mogelijkheid tot *interpersoonlijk contact* met de organisatie achter de ICT. Volgens de Gefen & Straub (2004) wordt vertrouwen via menselijke interactie opgebouwd en kan het vertrouwen in een ICT toenemen wanneer contact met een persoon achter de ICT mogelijk is. Gebruikers hebben bijvoorbeeld meer vertrouwen een website waarop zij contactinformatie kunnen vinden en foto's van medewerkers dan in een website waarop deze informatie ontbreekt. Tot slot lijkt het vertrouwen van een gebruiker in een ICT afhankelijk te zijn van *eerdere ervaringen* van de gebruiker met de organisatie achter de ICT. Gefen (2000) toonde in zijn studie aan dat positieve ervaringen met een bedrijf het vertrouwen van gebruikers in de ICT van dat bedrijf vergrootte.

2.2.5 Geïntegreerd model van factoren

Wanneer de factoren zoals geïdentificeerd in de voorgaande paragrafen gecombineerd worden, ontstaat het volgende beeld ten aanzien van de set van factoren die vertrouwen van gebruikers in ICT bepalen:

Figuur 4, Overzicht van factoren die van invloed zijn op het vertrouwen van gebruiker in ICT, TNO 2012

Zoals figuur 4 en voorgaande paragrafen laten zien, wordt het vertrouwen van gebruikers in ICT niet alleen bepaald door aan veiligheid gerelateerde factoren zoals de beveiliging van een ICT en de mate van misbruik, maar ook door factoren als gebruiksvriendelijkheid, mate van ervaring met ICT en algemeen maatschappelijk vertrouwen. Deze indirectere factoren zijn vaak 'zachter' in de zin dat ze moeilijker meetbaar zijn. Voor het monitoren van vertrouwen in ICT is daarom gekozen om sleutelvariabelen te identificeren die zo goed mogelijk meetbaar zijn. Sleutelvariabelen zijn bijvoorbeeld 'algemeen vertrouwen Nederlandse burger', 'ICT ervaringen van Nederlanders' en 'positieve/negatieve ervaringen met ICT'. Deze sleutelvariabelen komen in de hoofstukken 4 en 5 aan bod.

2.3 Het begrip 'Veiligheid van ICT'

Als een van de vitale infrastructuren vormt ICT de basis voor veel sociale en economische processen en innovaties, zeker waar het gaat om internet gerelateerde toepassingen. De keerzijde hiervan is dat de afhankelijkheid van de samenleving van deze infrastructuur steeds toeneemt, en de veiligheid en beschikbaarheid van de ICT infrastructuur van steeds vitaler belang wordt.

Maar wat bedoelen we eigenlijk als we het over "veiligheid van ICT" hebben? In de informatiebeveiliging wordt bij het uitwerken van het begrip meestal een driedeling gebruikt: ICT is veilig als aan eisen rond *beschikbaarheid*, *integriteit* en *exclusiviteit*[4] voldaan is:

- **Beschikbaarheid** is het garanderen dat informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor gebruikers (consumenten of bedrijven);

[4] In het Engels veelal Confidentiality, Integrity, Availability genoemd (CIA)

- **Integriteit** is het garanderen van het correct en volledig zijn van informatie en software;
- **Exclusiviteit** is het beschermen van gevoelige informatie tegen ongeautoriseerd gebruik.

In deze monitor zijn de verschillende indicatoren gestructureerd door ze in één van drie groepen te plaatsen die corresponderen met beschikbaarheid, integriteit en exclusiviteit. Hoewel de groepen in deze indeling – zoals bij elke indeling – een zekere overlap vertonen, is het een bruikbare manier om de indicatoren overzichtelijk in te delen. Hieronder worden de drie groepen indicatoren kort uitgewerkt.

2.4 Factoren die veiligheid van ICT bepalen

Meer dan bij vertrouwen in de veiligheid van ICT zijn de indicatoren rond de veiligheid van ICT gebonden aan specifieke technologie, en daarmee ook sterker tijdsgebonden. Bepaalde veiligheidsproblemen spelen bijvoorbeeld alleen bij specifieke apparatuur of communicatiemedia. De onderstaande indicatoren die iets zeggen over de veiligheid van ICT zijn daarom “bottom-up”, dus vanuit de problemen die in de praktijk spelen, opgesteld.

2.4.1 Beschikbaarheid

Onder beschikbaarheid wordt zoals genoemd verstaan het garanderen dat informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor gebruikers (consumenten of bedrijven). Dit betekent dat deze informatie en diensten niet alleen *online* zijn, maar ook dat de gebruikers er daadwerkelijk bij kunnen op de tijdstippen dat ze deze informatie en diensten nodig hebben. In de praktijk zijn voornamelijk twee problemen zichtbaar als het om de beschikbaarheid van ICT gaat:

- **Storingen** van apparatuur, software of netwerken kunnen resulteren in een volledige uitval van een dienst;
- **Distributed Denial Of Service (DDOS) aanvallen** overspoelen een server met berichten waardoor deze gedurende de aanval zeer traag wordt en niet meer beschikbaar is voor de bedoelde gebruikers.

2.4.2 Integriteit

Onder integriteit wordt zoals genoemd geschaard het garanderen van het correct en volledig zijn van informatie en software. Dit betekent ook dat informatie en software alleen gewijzigd mag worden door geautoriseerde partijen. In de praktijk zijn een aantal verschillende problemen mogelijk die de integriteit van ICT bedreigen:

- **Malware** is kwaadaardige software die gemaakt is door aanvallers om toegang te krijgen tot computersystemen, schade aan te richten of informatie te verzamelen;
- **Identiteitsfraude** treedt op als iemand (of software) zich voordoet als een andere persoon, en namens deze identiteit handelingen verricht (zoals e-mail versturen);
- **Website spoofing** is het namaken van een legitieme website met als doel gebruikers te misleiden;
- **Defacements** zijn het na een hack vervangen van een webpagina door een andere pagina die een andere boodschap heeft;
- **Illegale content** is het produceren, aanbieden, verspreiden en consumeren van illegale content. Het kan hierbij gaan om zeer ernstige misdrijven zoals bij kinderporno, maar ook om lichtere delicten zoals het aanbieden van content waarop copyright berust.

2.4.3 Exclusiviteit

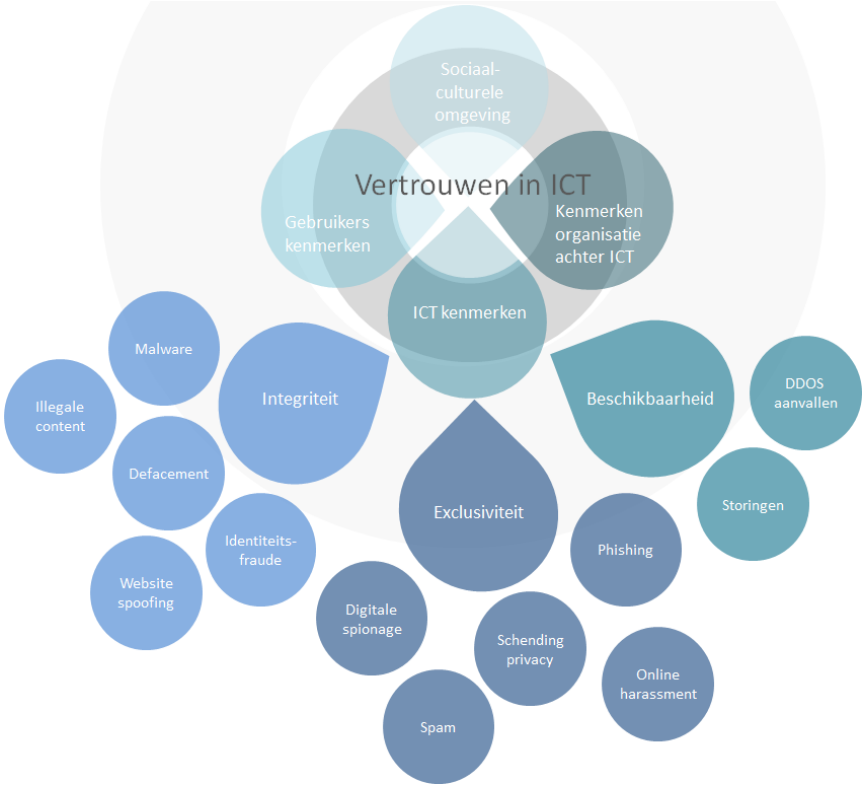
Onder exclusiviteit wordt zoals genoemd verstaan het beschermen van gevoelige informatie tegen ongeautoriseerd gebruik. Het garanderen van exclusiviteit heeft als een

van de voornaamste doelen het beschermen van de privacy van gebruikers, door hun persoonsgegevens tegen ongeautoriseerde toegang of gebruik te beschermen. In de praktijk zijn de volgende problemen zichtbaar als het om de exclusiviteit van ICT gaat:

- **Schending van de privacy** treedt op als ongeautoriseerde partijen toegang krijgen tot persoonsgegevens, of deze gegevens op een incorrecte wijze verzameld, gebruikt, gedeeld of bewaard worden;[5]
- **Online harassment** is het via digitale weg lastig gevallen worden, zoals bij stalking;
- **Spam** omvat het ontvangen van ongewenste berichten zoals massale reclame via e-mail;
- **Phishing** berichten (vaak e-mail) zijn is misleidende berichten die specifiek zijn opgesteld om aan een gebruiker geld, persoonsgegevens of andere zaken te ontfutselen;
- **Digitale spionage** is het zich toegang verschaffen tot gevoelige informatie middels digitale middelen, soms uitgevoerd door buitenlandse inlichtingendiensten.

2.4.4 Geïntegreerd model van factoren

Wanneer de genoemde factoren die de veiligheid van ICT (zoals hier geconceptualiseerd) bepalen gecombineerd worden, ontstaat het volgende beeld:



Figuur 5, Factoren (en indicatoren) die de veiligheid van ICT bepalen, TNO 2012

Deze factoren dienen bij de monitor als indicatoren waarmee in kaart gebracht wordt hoe de toestand rond de veiligheid van ICT in Nederland is voor consumenten en bedrijven. Als nieuwe factoren zichtbaar worden of oude factoren niet langer een rol van betekenis spelen zal dit model bijgesteld moeten worden.

[5] "Privacy" is een zeer breed begrip wat hier vrij nauw wordt uitgelegd. Onder privacy valt onder andere lichamelijke integriteit, de privacy van huis en haard, en veel andere zaken. Hier beperken we ons voornamelijk tot privacy voor zover dit betrekking heeft op de bescherming van persoonsgegevens, omdat juist dit sterk speelt bij veiligheid van ICT.

3 Methodologie

3.1 Onderdeel vertrouwen in ICT

Voor het onderdeel 'Vertrouwen in ICT' heeft een uitgebreide literatuurstudie plaatsgevonden naar factoren die vertrouwen van gebruikers in ICT beïnvloeden. Op basis van de factoren gevonden in de literatuur is een typologie gedefinieerd en een conceptueel model ontworpen. Per type factor zijn door de uitvoering van desk research zoveel mogelijk data verzameld over de huidige stand van zaken (bijv. de mate waarin gebruikers positieve of negatieve ervaringen hebben met ICT).

Op een aantal aspecten van 'vertrouwen in ICT' bleek weinig betrouwbare data beschikbaar. Om toch inzicht te krijgen in de mate waarin Nederlandse burgers vertrouwen in ICT hebben, heeft TNO een enquête uitgezet onder een representatieve steekproef van 1042 Nederlanders die met enige regelmaat van internet gebruik maken. Van deze steekproef waren 519 respondenten man en 523 vrouw.

Bij het uitzetten van de enquête is gestreefd naar een goede demografische spreiding over leeftijd en opleidingsniveau:

Leeftijdsgroep	Respondenten
18-24 jaar	126
25-34 jaar	145
35-44 jaar	227
45-54 jaar	223
55-64 jaar	200
65-75 jaar	121

Hoogste vorm van genoten onderwijs	Respondenten
LO (basisschool, lagere school, LAVO, VGLO)	24
LBO (VMBO basis/kader, LBO, LTS, ITO, LEAO, Huishoudschool, LLO)	146
MAO (VMBO GL/TL, MAVO, IVO, MULO, ULO, 3jr HBS, 3jr VWO, 3jr VHMO)	135
MBO (MTS, UTS, MEAO, ROC)	348
HAO (HAVO, VWO, Atheneum, Gymnasium, NMS, HBS, Lyceum)	87
HBO (HTS, HEAO, Wetensch. kand., Univers. onderwijs kand., Bachelor)	210
WO (Universitair onderwijs, Doctoraalopleiding, TH, Master)	92

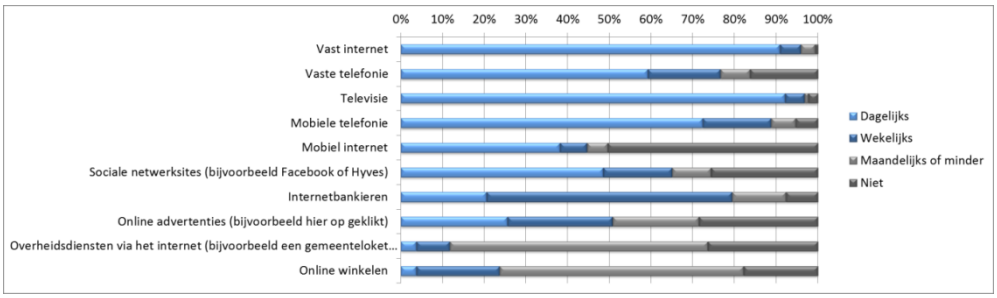
Om voldoende representativiteit te krijgen, zijn in de analyse de leeftijdscategorieën in drie groepen samengebracht (34 jaar en jonger, 35 – 54 jaar, en 55 en ouder). Hetzelfde geldt voor de opleidingsniveaus:

- Laag: LO, LBO, MAO
- Middel: MBO, HAO
- Hoog: HBO, WO

De enquête is met ondersteuning van de organisatie Survey Sampling International (SSI) afgenomen via het internet. De keuze voor een internetpanel betekent dat de antwoorden alleen representatief zijn voor dat deel van de bevolking wat daadwerkelijk internet gebruikt; anders zullen ze immers niet in staat zijn om deel te nemen aan een internetpanel. De Nederlanders die bijvoorbeeld helemaal niet van internet gebruik maken door een gebrek aan vertrouwen in ICT blijven hierdoor buiten beeld. Dit was helaas onvermijdelijk, omdat het vinden en interviewen van een (representatieve) groep die

internet niet gebruikt meer kosten met zich mee zou brengen dan haalbaar is binnen het kader van deze studie.

Van de respondenten is ook in kaart gebracht hoe vaak ze van een aantal op ICT gebaseerde diensten gebruik maken:



Figuur 6 - "Hoe vaak heeft u de afgelopen 6 maanden van onderstaande diensten gebruik gemaakt?"

Bron: TNO enquête Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

De vragenlijst is opgesteld met als doel om twee variabelen in kaart te brengen, namelijk: "Vertrouwen in veiligheid van ICT door Nederlandse burgers" en "Veiligheid van ICT gebruik van Nederlandse burgers" (waaronder gerekend de exclusiviteit, integriteit en beschikbaarheid van informatie en diensten). Deze variabelen zijn meetbaar gemaakt door specifieke indicatoren te formuleren, welke in een serie meerkeuzevragen getoetst zijn:

Variabele	Indicator
Vertrouwen in veiligheid van ICT door Nederlandse burgers	Frequentie waarin de respondent zich zorgen maakt over veiligheidsrisico's bij internetgebruik.
	Activiteiten op internet waar respondent van afgezien heeft door zorgen over veiligheid.
	Diensten op internet waar respondent van afgezien heeft door zorgen over veiligheid.
	Mate waarin respondent denkt aanbieders van ICT diensten te kunnen vertrouwen.
Veiligheid van ICT gebruik van Nederlandse burgers	Door respondent aangegeven ervaringen met problemen rond veiligheid van internetgebruik.
	Omvang van financiële of andere schade die respondent denkt geleden te hebben door problemen rond veiligheid van internetgebruik.
	Welke ICT-diensten respondent niet heeft kunnen gebruiken door een storing.
	Welke software hulpmiddelen die respondent gebruikt om de eigen computer te beschermen.
	Frequentie waarin respondent back-ups maakt van documenten.

Uit de enquête komt ook een aantal inzichten voort dat betrekking heeft op de context waarin burgers (on)veiligheid van ICT ervaren. Deze uitkomsten van de enquête worden, waar relevant, in dit rapport gepresenteerd en aangehaald.

3.2 Onderdeel veiligheid van ICT

Om te komen tot een overzicht van relevante indicatoren voor de veiligheid van ICT zijn verschillende studies over cybersecurity en -crime bestudeerd. Indicatoren genoemd in deze studies zijn verzameld en aangevuld door verschillende experts op het onderwerp. Per indicator zijn zo recent mogelijke data verzameld.

Belangrijk is het om hierbij te vermelden dat het zeer moeilijk is gebleken om betrouwbare statistieken op het onderwerp veiligheid van ICT te genereren. Indicatoren voor de veiligheid van ICT betreffen vaak data over de mate waarin cybercrime voorkomt. Het probleem met het in kaart brengen van cybercrime is dat het weinig zichtbaar is (omdat criminelen zo onzichtbaar mogelijk opereren). Daarbij wordt niet altijd melding gemaakt of aangifte gedaan van voorvallen van cybercrime (door bedrijven niet vanwege angst voor reputatieschade en door personen niet omdat het vaak gaat om relatief kleine bedragen).

De cijfers die wel voorhanden zijn, worden veelal gegenereerd door bedrijven die op het gebied van cybersecurity diensten of producten leveren (bijv. consultancy of softwareproducten). Omdat bedrijven belang hebben bij een zekere mate van onveiligheid bestaat er de kans zij de gegevens niet objectief interpreteren. Daarnaast blijken samples genomen door bedrijven om onveiligheid in kaart te brengen niet altijd representatief te zijn voor de target populatie. Ook bestaat vaak onduidelijkheid over de door bedrijven gehanteerde definities en toegepaste methoden en technieken die aan onderzoek ten grondslag liggen. Dit maakt het moeilijk voor TNO om de kwaliteit van de data in te schatten.

De gepresenteerde data in dit rapport kunnen dan ook niet anders begrepen worden dan als indicaties van de veiligheid van ICT en moeten met alle voorzichtigheid benaderd worden.

4 Vertrouwen in ICT

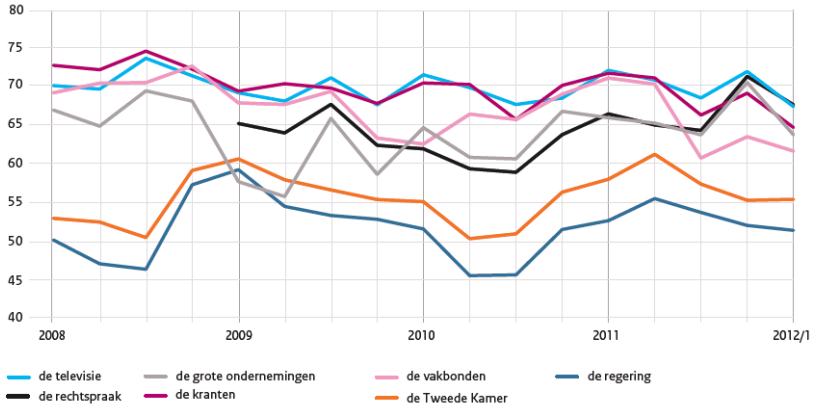
In hoofdstuk 2 werd een model geïntroduceerd waarin de factoren die van invloed zijn op het vertrouwen van gebruiker in ICT samengebracht zijn. De indicatoren die het vertrouwen van gebruikers in ICT aangeven worden in dit hoofdstuk met behulp van de beschikbare data in kaart gebracht aan de hand van deze vier groepen: de sociaal-culturele omgeving van de gebruiker, kenmerken van de gebruiker zelf, kenmerken van ICT en kenmerken van de organisatie achter een ICT dienst.

4.1 Sociaal-culturele omgeving

4.1.1 Algemeen vertrouwen Nederlandse burger

Verschillende onderzoeken geven een empirische basis voor een positieve correlatie tussen 'algemeen vertrouwen' in een land en het vertrouwen in en adoptie van ICT. Hoe groter het vertrouwen in instituties en medeburgers is, des te groter het vertrouwen in de ICT van instituties en de online interactie (bijv. online zaken doen) met anderen. Verschillende studies wijzen op een relatief hoog en stabiel vertrouwensniveau in Nederland (in vergelijking met andere landen). Het Sociaal en Cultureel Planbureau (2012/1:9) bracht bijvoorbeeld het vertrouwen van Nederlanders in zeven instituties over de afgelopen 4 jaar (2008-2012) in kaart (zie Figuur 7)[6]. Hieruit blijkt dat tussen 2008 en 2012 het vertrouwen van Nederlanders in Nederlandse instituties gemiddeld 63% was en fluctueerde met 11%.

[6] De zeven instituties onderzocht zijn: televisie, rechtspraak, grote ondernemingen, kranten, vakbonden, Tweede Kamer en regering.



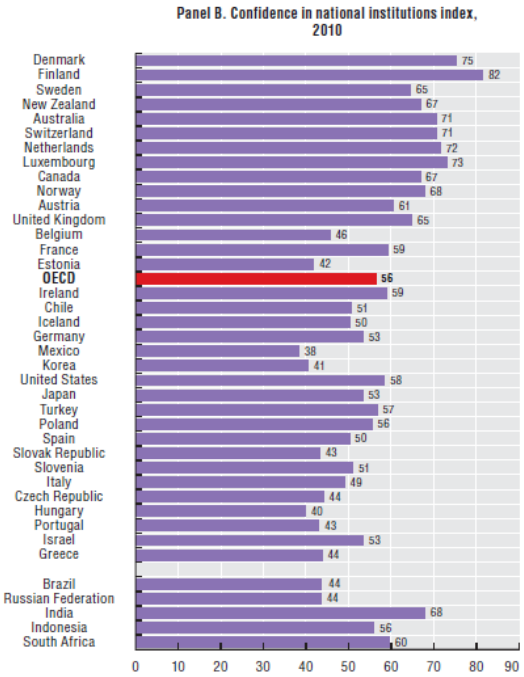
a Vermeld zijn percentages scores 6-10 op een schaal van 1 (geen enkel vertrouwen) tot 10 (alle vertrouwen) in antwoord op de vraag 'Hoeveel vertrouwen heeft u op dit moment in de volgende instellingen in Nederland?'.

Figuur 7, vertrouwen in zeven instituties, bevolking van 18+, 2008-2012 (in procenten), Bron: SCP, COB 2008/1-2012/1

Van de 7 instituties die onderdeel uitmaken van het onderzoek hebben Nederlanders het minst vertrouwen in de regering (gemiddeld 52% in de periode van 2008-2012) en het meest vertrouwen in kranten en de televisie (beiden gemiddeld 70% in de periode van 2008-2012). Het vertrouwen in grote ondernemingen (relevant in verband met vertrouwen in online zaken doen) was in de periode 2008-2012 gemiddeld 64%. Het hoogste vertrouwen hadden Nederlanders in de kranten in het tweede kwartaal van 2008 (74,5%) en het laagste vertrouwen in de regering in het tweede kwartaal van 2010 (45,5%). Meest stabiel was de afgelopen 4 jaar het vertrouwen in de televisie, welke een fluctuatie van 7% kende. Het meest onstabiel was het vertrouwen in grote ondernemingen, welke een fluctuatie van 15% kende. Deze fluctuatie van het vertrouwen in ondernemingen (met een dieptepunt in 2009) kan verklaard worden door de financiële crisis en de DSB-affaire (SCP, 2009/1:4).

Wanneer Nederland vergeleken wordt met andere landen, lijkt het vertrouwen dat Nederlanders in nationale instituties hebben relatief hoog. Uit het onderzoek 'Society at a Glance' van de OECD (2011:92) onder burgers van verschillende landen blijkt dat in 2010 72% van de Nederlanders vertrouwen had in nationale instituties - bestaande uit defensie, de rechtspraak en de nationale overheid[7]. Gemiddeld was het vertrouwen in nationale instituties van burgers van landen die deelnamen aan het onderzoek 56%.

[7] Cijfers uit 2011 (Society at a Glance 2012) waren nog niet beschikbaar op het moment dat dit rapport werd geschreven.



Figuur 8, percentage vertrouwen in nationale instituties (defensie, rechtspraak, nationale overheid) 2010, Bron: OECD, Society at a Glance, 2011

Daarnaast lijkt het merendeel van de Nederlanders vertrouwen te hebben in anderen. Vertrouwen in anderen is relevant als het ICT aangaat, omdat via ICT veelal interactie met anderen plaatsvindt (denk bijvoorbeeld aan het online zaken doen via Marktplaats of sociale interactie via sociale media). Onderzoek van het Sociaal en Cultureel Planbureau (2012/1:35) bracht voor het eerste kwartaal van 2012 verschillende vertrouwenstypen in kaart, waaronder het vertrouwen van mensen in anderen (zie Figuur 9). 61% van de referentiegroep is het eens met de stelling: 'Over het algemeen zijn de meeste mensen wel te vertrouwen'.

	allen	vol vertrouwen	behoedzaam	wantrouwig
'Ik heb het gevoel dat ik weinig grip heb op mijn eigen toekomst': eens	28	0	44	45
'In het algemeen word ik eerlijk behandeld': eens	74	90	79	28
'Over het algemeen zijn de meeste mensen wel te vertrouwen': eens	61	81	67	4
'Je kunt niet voorzichtig genoeg zijn in de omgang met mensen': eens	39	6	45	90
aandeel in de bevolking	100%	37%	45%	18%

a De groepen zijn onderscheiden door middel van k-means clustering van de oorspronkelijke vijf antwoordmogelijkheden (zeer mee oneens – zeer mee eens). Zie het tekstkader over segmentering voor een toelichting.

Figuur 9, vertrouwenstypen, bevolking van 18+, 2011-2012 (in procenten), Bron: SCP, COB 2012/1

Ook in 2008 kwam het SCP op een percentage van 61% van de Nederlanders dat anderen vertrouwt (zie Figuur 10) en in 2004 kwam de Europese Commissie op basis van haar European Social Survey op eenzelfde percentage van 61% (zie Figuur 11). Het lijkt dus dat het vertrouwen in anderen over de afgelopen 8 jaar stabiel was.

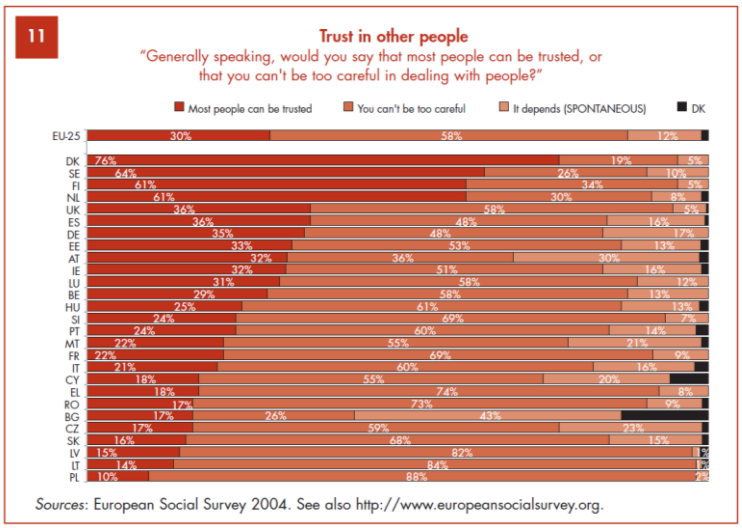
Tabel 2.2 Enkele opvattingen over de samenleving, bevolking van 18+, eerste kwartaal 2008 (in procenten)[a]

	(zeer) oneens	(zeer) eens
over het algemeen zijn de meeste mensen wel te vertrouwen	11	61
je kunt niet voorzichtig genoeg zijn in de omgang met mensen	25	39
er zijn nog altijd veel mensen die bereid zijn om een ander te helpen	4	81
in ons land gaan de mensen met steeds minder respect met elkaar om	7	72
in ons land is er te weinig aandacht voor mensen die het minder hebben	19	57
de mensen in ons land moeten meer zelf verantwoordelijk zijn en minder rekenen op overheidsvoorzieningen	25	49
Nederland zou een prettiger land zijn als er minder immigranten zouden wonen	33	38
de aanwezigheid van verschillende culturen is winst voor onze samenleving	26	41
het Nederlands lidmaatschap van de EU is een goede zaak	18	44
mensen zoals ik ondervinden vooral nadelen van het verdwijnen van de grenzen en het meer open worden van onze economie	44	17

a De stellingen worden voorgelegd met vijf antwoordmogelijkheden van 'zeer mee oneens' tot 'zeer mee eens' en 'ik weet het niet'; de gepresenteerde percentages tellen met 'neutraal' en 'ik weet het niet' op tot 100%.

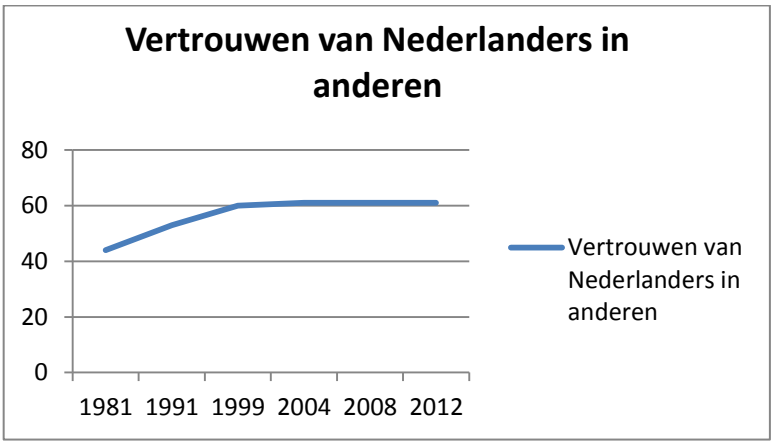
Bron: COB 2008/1

Figuur 10, opvattingen over samenleving, bevolking van 18+, 2008 (in procenten), Bron: SCP, COB 2008/1-2012/1



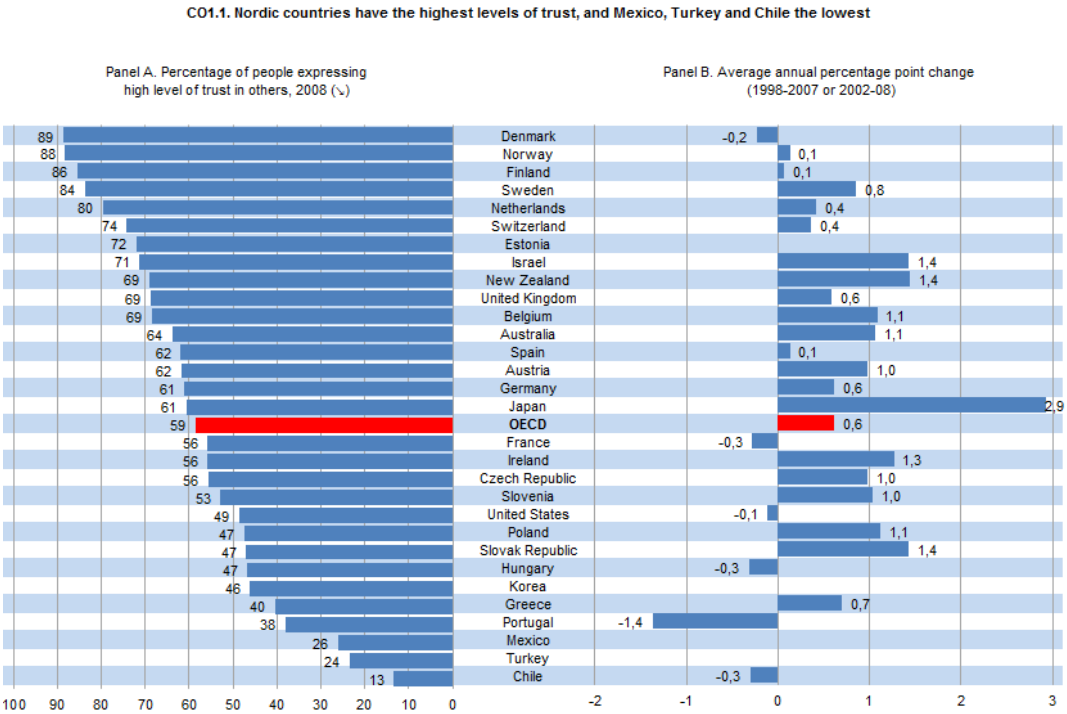
Figuur 11, vertrouwen in anderen, 2004 (in procenten), Bron: European Social Survey

Om de stabiliteit van vertrouwen van Nederlanders in anderen nader historisch in kaart te brengen kunnen de cijfers worden gebruikt van de Wold Value Survey, welke het vertrouwen van burgers in medeburgers in 4 'waves' in 1981, 1991, 1999 en 2006 heeft gemeten in ongeveer 30 landen. Onderstaande Figuur 12 laat zien dat er in de jaren 90 een stijging van vertrouwen in anderen plaatsvond en dat het sinds 2000 stabiel is gebleven.



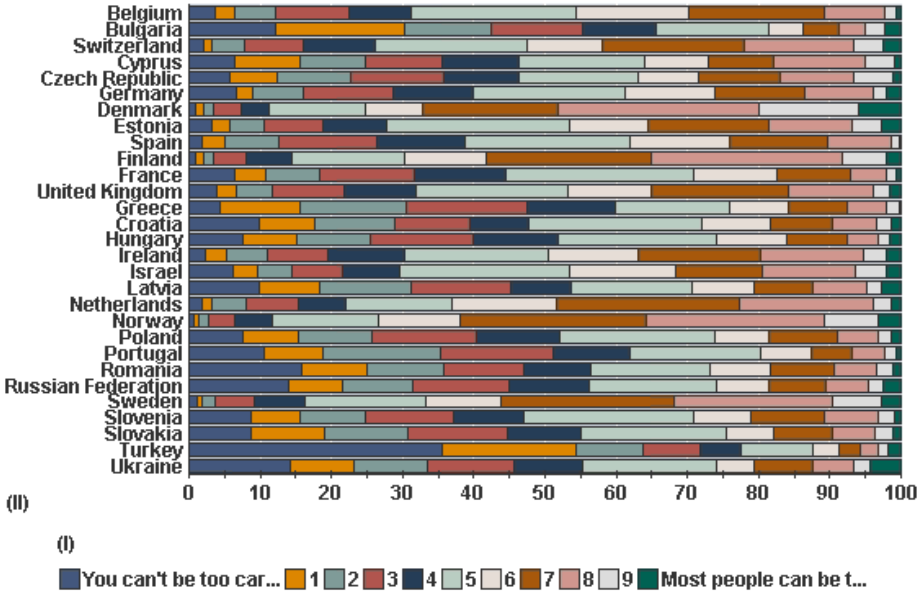
Figuur 12, Percentage Nederlanders dat vertrouwen heeft in anderen, periode 1981-2012, gebaseerd op cijfers van Wold Value Survey, European Social Survey en COB van SCP

Internationaal gezien, lijkt het percentage Nederlanders dat anderen vertrouwt relatief hoog. In haar studie uit 2011 gaf de OECD aan dat het percentage burgers dat een groot vertrouwen in anderen heeft in 2008 in Nederland 80% was (zie Figuur 8).



Figuur 13, Percentage burgers dat in 2008 een groot vertrouwen in anderen had, Bron: OECD Society at a Glance 2011,

Wel lijken de cijfers van de OECD structureel hoger te liggen dan de cijfers van World Value Survey, European Social Survey en Sociaal Cultureel Planbureau. Zowel de World Value Survey als de European Social Survey laten in alle landen lagere vertrouwenscijfers zien (tussen de 10 en 20% lager). Ter vergelijking: in 2008 kwam de European Social Survey op een percentage van 63% van de Nederlanders dat anderen vertrouwt (zie Figuur 14 hieronder).



Figuur 14, Percentage burgers dat in 2008 een groot vertrouwen in anderen had, Bron: European Social Survey,

Over het algemeen kan gesteld worden dat het vertrouwen van Nederlandse burgers in instituties en elkaar sinds de jaren 80 met ongeveer 10 tot 15% is toegenomen en daarna stabiel is gebleven. Hiermee lijkt op het moment een relatief stabiel en gedegen vertrouwensomgeving te zijn waarin ICT wordt gebruikt. Zoals gezegd is de sociaal-culturele omgeving slechts één van de aspecten van invloed op vertrouwen in ICT.

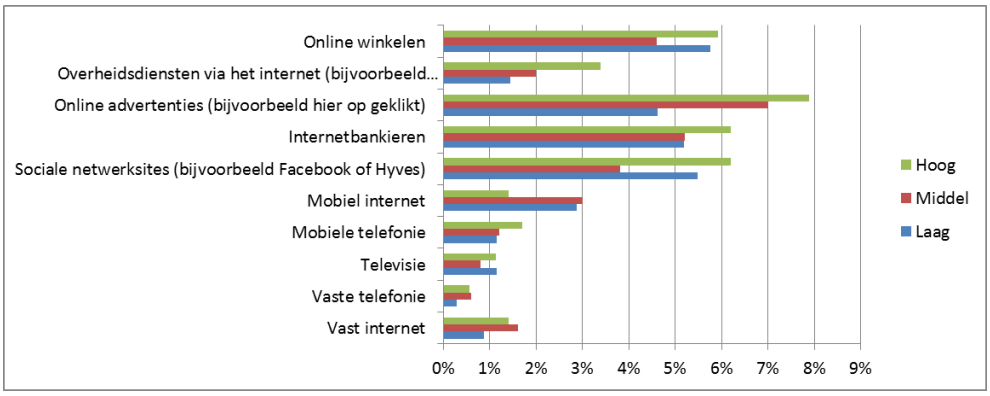
4.2 Gebruikerskenmerken

4.2.1 *Vertrouwen en demografische kenmerken*

De TNO enquête onder 1042 Nederlanders had een afdoende omvang om in de antwoorden onderscheid te kunnen maken op leeftijd, sekse of opleidingsniveau van de respondenten.

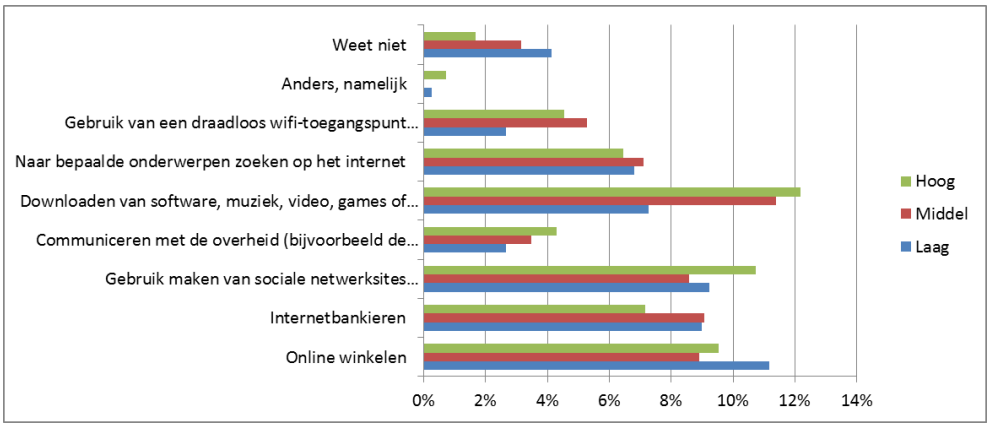
Bij analyse van de resultaten zijn er geen significante verschillen tussen mannen en vrouwen gevonden. Dit betekent dat we op basis van deze gegevens geen reden hebben om aan te nemen er wezenlijke verschillen zijn tussen het vertrouwen in ICT door mannen of vrouwen.

De volgende figuren laten zien dat tussen de opleidingsniveaus wel enige verschil zit in de mate waarin mensen ICT (-diensten) vertrouwen, al zijn deze verschillen klein:



Figuur 15, "Heeft u in de afgelopen 6 maanden een van de onderstaande diensten niet gebruikt omdat u de veiligheid van de dienst niet vertrouwde?"

Bron: TNO enquête Veiligheid en Vertrouwen in ICT 2012 ((N^{hoog} = 302, N^{middel} = 435, N^{laag} = 305))

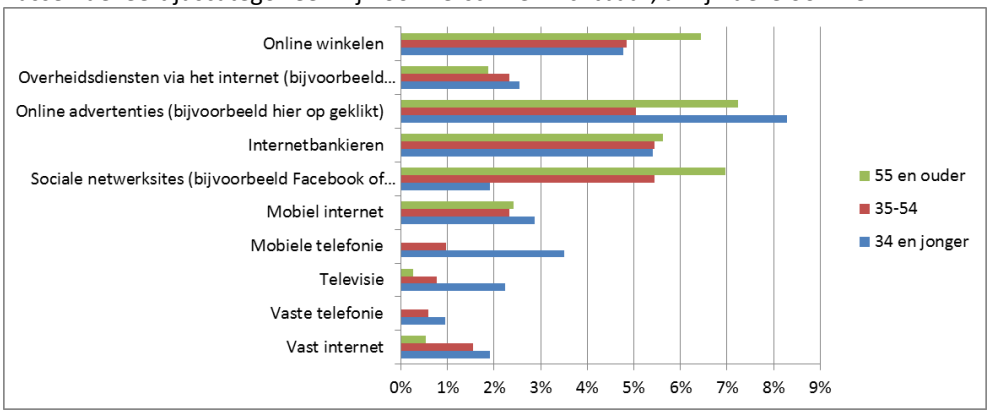


Figuur 16, "Hebben zorgen over veiligheid u doen afzien van de volgende activiteiten in de afgelopen 6 maanden?"

Bron: TNO enquete Veiligheid en Vertrouwen in ICT 2012 (N^{hoog} = 302, N^{middel} = 435, N^{laag} = 305)

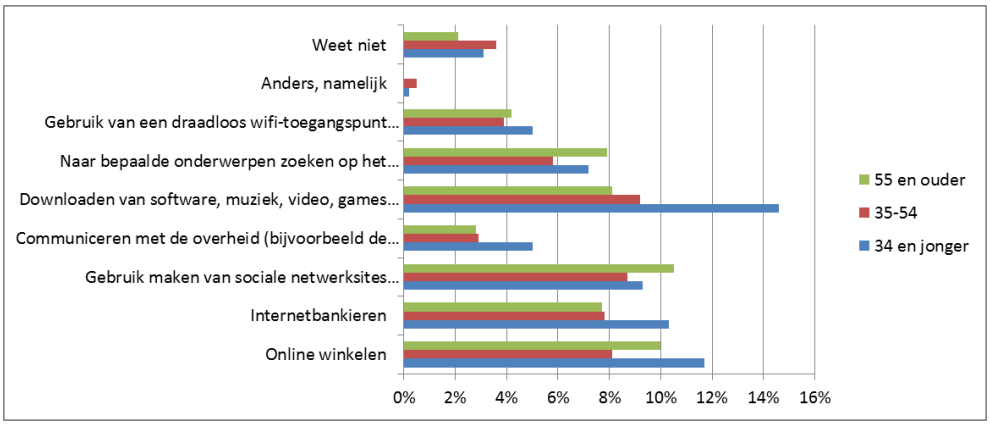
In de bovenstaande grafieken betreffen de verschillen slechts enkele procenten. Bij het downloaden lijken hoger opgeleiden zich bijvoorbeeld wat meer zorgen te maken om hun veiligheid van lager opgeleiden, en hetzelfde geldt voor online advertenties. De verschillen zijn echter klein, en kunnen voor een deel ook veroorzaakt zijn door verschillen in de wijze waarop mensen met verschillende opleidingsniveaus de vragen interpreteren. Om een goed inzicht te krijgen in de wijze waarop opleidingsniveau en vertrouwen in veiligheid van ICT samenhangen is diepgaander onderzoek nodig.

Tussen de leeftijdscategorieën zijn ook verschillen zichtbaar, al zijn deze ook klein:



Figuur 17, "Heeft u in de afgelopen 6 maanden een van de onderstaande diensten niet gebruikt omdat u de veiligheid van de dienst niet vertrouwde?"

Bron: TNO enquete Veiligheid en Vertrouwen in ICT 2012 ($N^{34\ en\ jonger}$=271, N^{35-54}=450, $N^{55\ en\ ouder}$ 321)



Figuur 18, "Hebben zorgen over veiligheid u doen afzien van de volgende activiteiten in de afgelopen 6 maanden?"

Bron: TNO enquête Veiligheid en Vertrouwen in ICT 2012 ($N^{34\ en\ jonger}$=271, N^{35-54}=450, $N^{55\ en\ ouder}$ 321)

Opvallend hierbij is dat waar een klein percentage respondenten van 34 en jonger bij mobiele telefonie, televisie of vaste telefonie aangaf dit niet gebruikt te hebben wegens zorgen om veiligheid, deze zorgen bij respondenten van 55 en ouder vrijwel niet aanwezig waren.

4.2.2 *Ervarenheid in ICT gebruik*

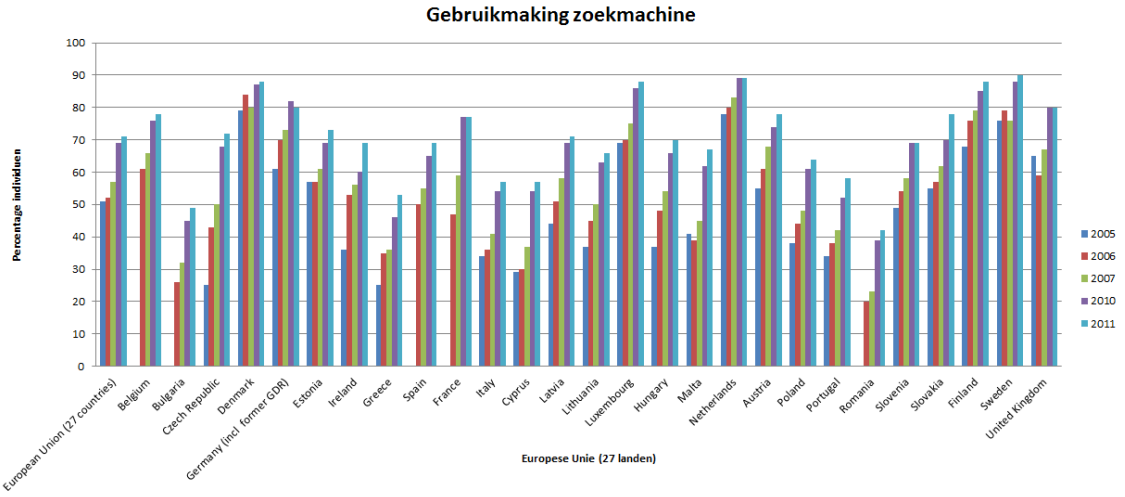
Een andere factor die van invloed is op het vertrouwen van gebruikers in ICT, is hun ervarenheid met het gebruik van ICT. Zoals beschreven in hoofdstuk 2, neemt eerst het vertrouwen toe naarmate de ervaring van de gebruiker groter wordt en daarna (bij zeer ervaren gebruikers) weer af. Afnemend vertrouwen van expert gebruikers heeft te maken met het feit dat zij beter op de hoogte zijn van de zwakke onderdelen van een ICT. Toenemend vertrouwen van onervaren ten opzichte van een 'basis' gebruiker heeft te maken met het feit dat basis gebruikers meer vertrouwd zijn en zich daardoor meer vertrouwd voelen met de ICT (bijvoorbeeld specifieke user interfaces). De volgende Tabel 2 met data van Eurostat laat zien dat Nederlanders net iets bovengemiddeld scoren als het gaat om basisvaardigheden (zoals het kopiëren van folders, het gebruiken van spreadsheets en het maken van presentaties) en iets lager als het gaat om meer geavanceerdere vaardigheden (zoals het schrijven van een computerprogramma).

Computer skills of individuals, 2011
% all individuals

	Copied or moved a file or folder		Used basic arithmetic formulas in a spreadsheet		Created electronic presentations		Written a computer program	
	Aged 16-74	Aged 16-24	Aged 16-74	Aged 16-24	Aged 16-74	Aged 16-24	Aged 16-74	Aged 16-24
EU27	**63**	**89**	**43**	**67**	**31**	**59**	**10**	**20**
Belgium	68	92	46	67	35	70	11	20
Bulgaria	41	76	22	47	6	18	2	5
Czech Republic	60	89	43	74	18	42	5	11
Denmark	79	95	67	88	50	88	11	19
Germany	72	94	44	60	33	67	9	18
Estonia	59	91	47	75	25	48	9	21
Ireland	60	82	44	54	21	36	9	(13)
Greece	47	88	34	65	23	55	8	17
Spain	58	84	41	66	33	66	12	27
France	67	85	49	74	38	63	11	17
Italy	54	85	35	61	23	50	9	18
Cyprus	53	92	41	77	29	65	6	12
Latvia	61	97	46	87	32	75	7	18
Lithuania	57	97	42	82	29	68	8	20
Luxembourg	80	96	62	73	50	75	16	(21)
Hungary	63	92	48	81	20	45	11	25
Malta	59	93	44	74	30	63	8	(21)
Netherlands	81	95	54	63	55	89	9	12
Austria	75	99	56	87	43	84	13	30
Poland	52	94	33	70	16	47	6	16
Portugal	57	96	42	78	32	78	7	18
Romania	38	72	20	46	8	18	6	16
Slovenia	61	97	48	85	36	85	6	(16)
Slovakia	70	95	52	77	23	54	6	13
Finland	77	95	61	76	52	84	26	37
Sweden	73	88	61	67	51	72	24	34
United Kingdom	72	94	51	72	36	61	13	25
Iceland	82	94	73	86	55	88	15	20
Norway	68	89	67	85	61	86	18	(20)

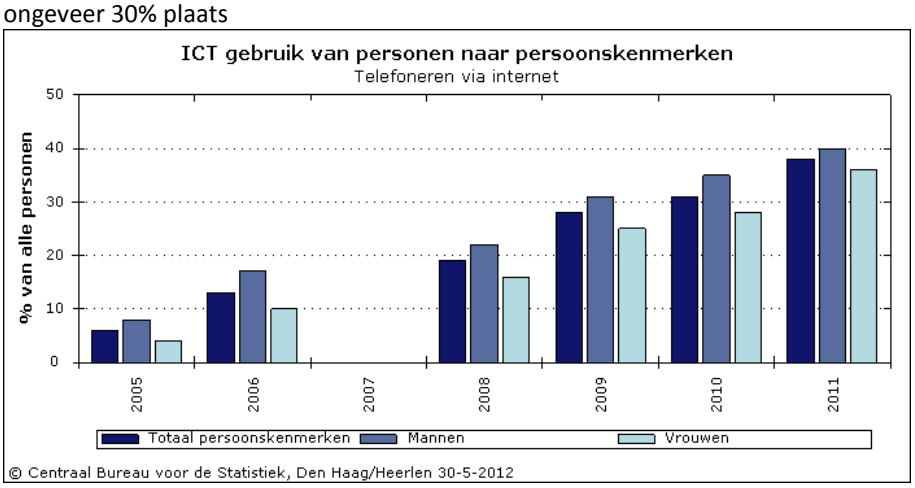
Tabel 2, Computer vaardigheden van individuen in 2011, Bron: Eurostat.

Daarnaast laat Figuur 19 zien dat Nederland ruim boven het Europese gemiddelde zit als het gaat om een basisvaardigheid als de gebruikmaking van zoekmachines op het Internet (in 2011 maakte 89% van de Nederlanders regelmatig gebruik van een zoekmachine; het Europese gemiddelde was 71%).



Figuur 19, Gebruikmaking zoekmachine door individuen 2005-2011, Bron: Eurostat.

Dat Nederlanders daarnaast steeds vaardiger worden in het gebruik van complexere applicaties die via het Internet beschikbaar zijn blijkt uit Figuur 20, welke een overzicht geeft van het telefoneren via Internet door Nederlanders over de afgelopen 7 jaar. Tussen 2005 en 2011 vond er een toename van het gebruik van telefoneren via internet van ongeveer 30% plaats

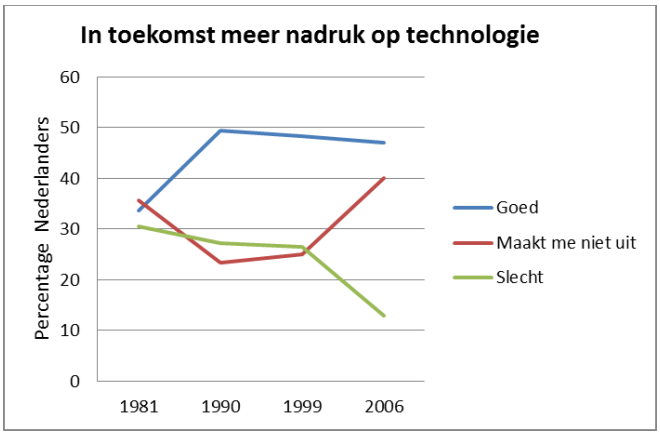


Figuur 20, Telefoneren via het Internet door Nederlanders 2005-2011, Bron: CBS.

Over het algemeen lijkt een relatief groot deel van de bevolking van Nederland over weg te kunnen met makkelijke en iets complexere applicaties beschikbaar via het Internet. De gepresenteerde cijfers wijzen op een bovengemiddelde vertrouwdheid van Nederlandse gebruikers met gangbare ICT applicaties.

4.2.3 *Eerdere ervaringen met ICT*

Een derde gebruikers-gerelateerde factor die van invloed is op het vertrouwen van gebruikers in ICT zijn hun ervaringen met ICT. Statistieken wijzen erop dat de meeste Nederlanders positieve ervaringen hebben en technologieën positief waarderen. Historisch gezien is dit niet altijd het geval geweest. Cijfers van het World Values Survey wijzen er bijvoorbeeld op dat technologieën in de jaren 80 minder positief werden ervaren dan in de jaren 90 en 2000. Figuur 21 laat zien dat in 1981 30,6% negatief antwoordde op de vraag "Zou in de toekomst meer nadruk op technologie moeten komen te liggen?" terwijl dit in 2006 12,9% was[8].

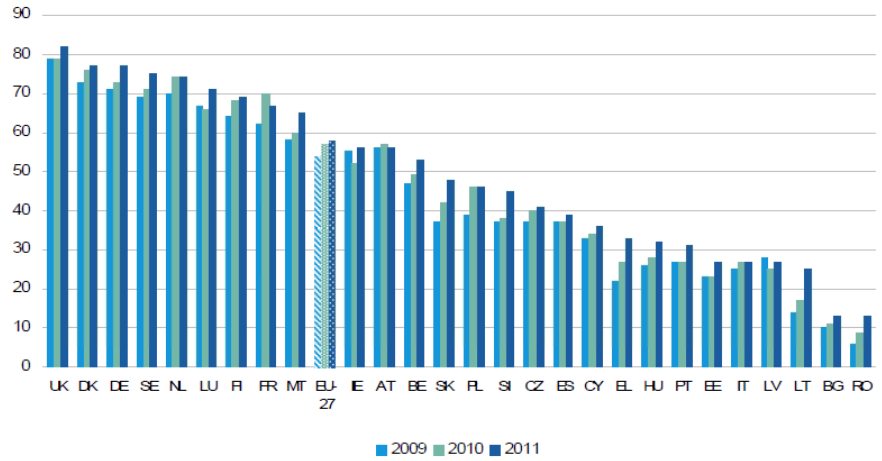


Figuur 21, Percentage individuen dat in toekomst meer nadruk op technologie wil, Bron: World Values Survey.

[8] Cijfers uit 2011 van de World Values Survey (sixth wave) waren op het moment dat dit rapport geschreven werd nog niet beschikbaar.

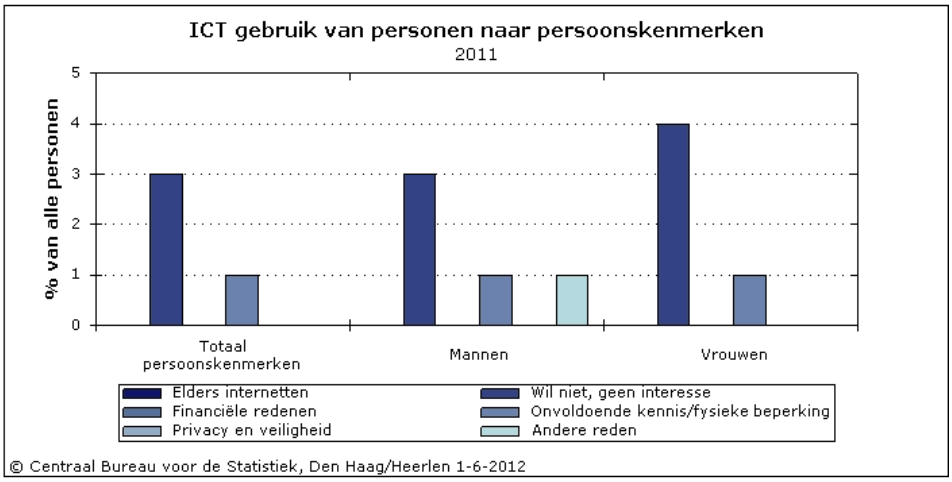
Ook de gebruikerscijfers lijken erop te wijzen dat ervaringen van Nederlanders met ICT over het algemeen positief zijn. De volgende Figuur 22 laat bijvoorbeeld zien dat Nederland tot de Europese top 5 van landen behoort waarvan burgers online inkopen doen. Het doen van online inkopen is één van de activiteiten (naast bijvoorbeeld e-banking) waarbij risico's voor de gebruiker (en mogelijkheid tot negatieve ervaringen) relatief hoog zijn (denk aan misbruik persoonlijke gegevens of het niet krijgen van een dienst/product of verkeerde dienst/product). Het lijkt erop dat de belangen van Nederlanders bij het doen van online inkopen weinig worden geschaad of dat eventuele negatieve ervaringen hen er niet van weerhouden om online inkopen te doen.

Figure 8: Internet users who bought or ordered goods or services for private use over the internet in the last 12 months, 2009-2011 (% of internet users)



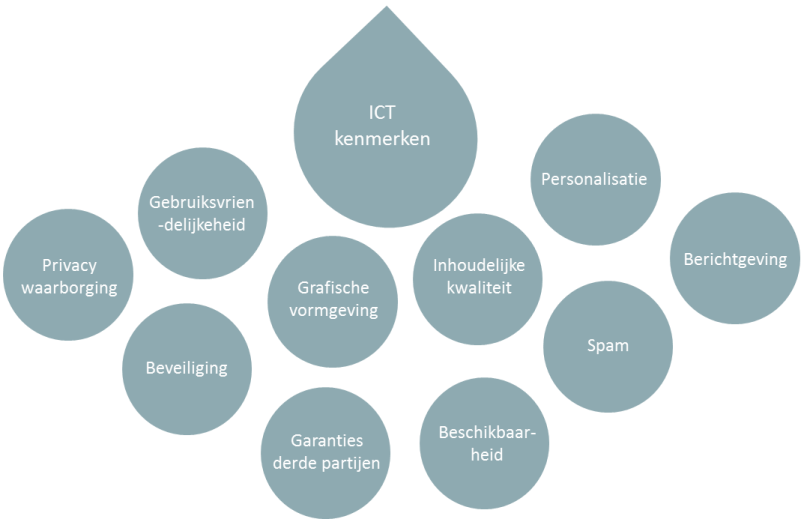
Figuur 22, Percentage internet gebruikers dat online goederen of diensten bestelden, 2009-2011, Bron: Eurostat.

Figuur 23, gebaseerd op data van het CBS, geeft het percentage Nederlanders weer welke in 2011 geen gebruik maakten van ICT om privacy c.q. veiligheidsredenen. Geen van de respondenten gaf aan ICT niet te gebruiken om privacy of veiligheidsredenen, 3% van de mannelijke en 4% van de vrouwelijke respondenten gaven aan ICT niet te gebruiken vanwege gebrek aan interesse. 1% van de mannen en 1% van de vrouwen gaven aan ICT niet te gebruiken vanwege onvoldende kennis en/of fysieke beperking(en) en 1% van de mannen gaf een andere reden op om ICT niet te gebruiken. De cijfers van het CBS laten daarnaast zien dat van 2005 tot en met 2011 alleen in het jaar 2007 respondenten privacy en veiligheid als reden opgaven om ICT niet te gebruiken, namelijk 1% van de mannelijke respondenten.



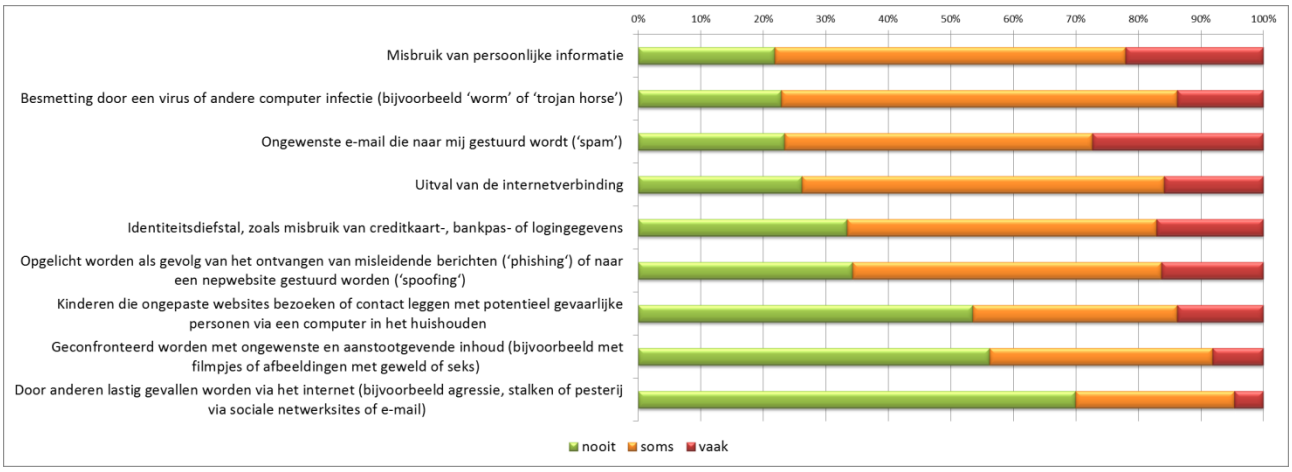
Figuur 23, 2011, Percentage individuen dat ICT niet gebruikt om specifieke reden, Bron: CBS.

4.3 ICT kenmerken



De resultaten van de voor dit onderzoek uitgevoerde enquête onder een representatieve steekgroep van Nederlandse burgers geven enig inzicht in de mate waarin de verschillende ICT kenmerken een rol spelen bij het vertrouwen van mensen in ICT. ICT kenmerken die (volgens de literatuurstudie zoals uitgevoerd in 2.2) van invloed kunnen zijn op vertrouwen in ICT zijn bijvoorbeeld de beveiliging van de ICT, geboden privacy waarborgen en mate van beschikbaarheid van de ICT (voor een volledig overzicht zie paragraaf 2.2). In deze paragraaf bespreken we de resultaten van de enquête per vraag.

Eén van de vragen uit de enquête betrof de frequentie waarmee Nederlanders zich zorgen maken over specifieke problemen (e.g. virusbesmetting, misbruik van gevens) bij het gebruik van ICT.



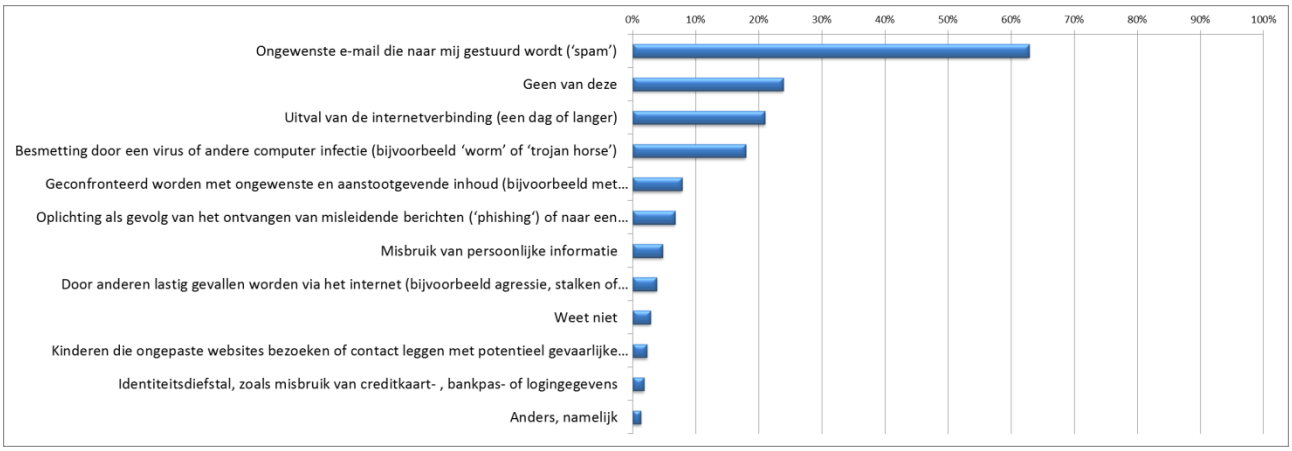
Figuur 24, "Hoe vaak maakt u zich zorgen over de volgende mogelijke problemen rond privé-internetgebruik?"

Bron: TNO enquête Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

Hierbij is het belangrijk om te benadrukken dat de vraagstelling zich richt op de *frequentie* waarin mensen zich zorgen maken, en niet de (subjectieve en dus moeilijk te meten) *zwaarte* van deze zorgen. Het kan dus zijn dat iemand zich soms ernstige zorgen maakt, of dat iemand zich vaak lichte zorgen maakt.

Opvallend is dat de respondenten aangeven dat ze zich relatief weinig zorgen maken over problemen die gerelateerd zijn aan online lastig gevallen worden (geconfronteerd worden met ongewenste inhoud, door anderen lastig gevallen worden). Waar de respondenten zich voornamelijk zorgen om lijken te maken is besmetting van de computer door een virus, het ontvangen van Spam, of misbruik van hun persoonlijke informatie (waaronder ook identiteitsdiefstal valt). Tot slot scoort de factor met betrekking tot zorgen over het uitvallen van de internetverbinding opvallend hoog.

Interessante is om de voorgaande vraag over zorgen over ICT gerelateerde problemen te confronteren met daadwerkelijk ervaren problemen. De volgende grafiek geeft inzicht in de daadwerkelijk ervaren (typen) problemen door respondenten.

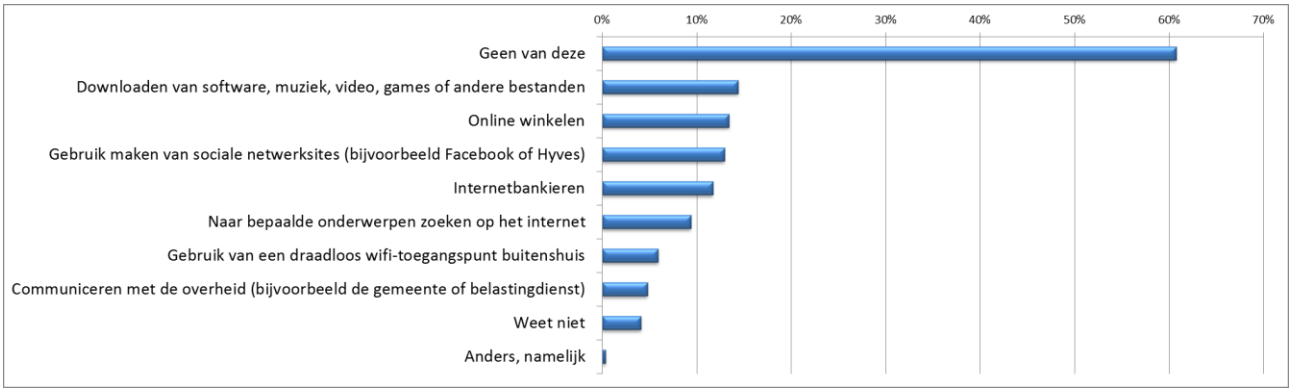


Figuur 25, "Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?"

Bron: TNO enquête Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

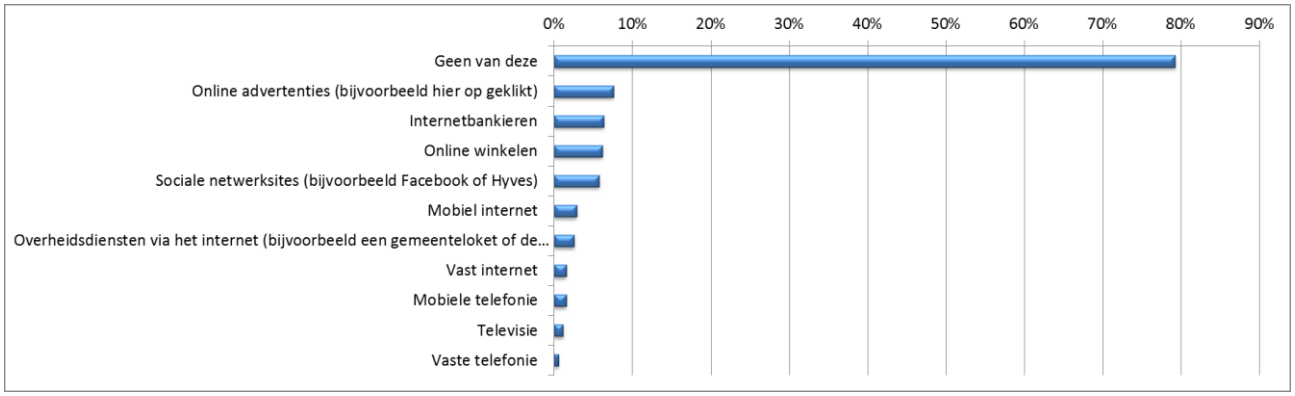
De eerder gesignaleerde zorgen over virussen, Spam en uitval van de internetverbinding lijken samen op te gaan met het relatief vaak ervaren van deze problemen. Opvallend is echter dat als het over misbruik van persoonsgegevens gaat, dit niet het geval is. Hier laten de twee voorgaande grafieken verschillen zien in de zin dat respondenten aangegeven zich regelmatig zorgen te maken over misbruik van persoonsgegevens (21%), maar dit relatief weinig meemaken (5%).

Een andere indicatie van de mate waarin burgers ICT vertrouwen is de vraag of ze een dienst of ICT daadwerkelijk niet gebruikt hebben omdat ze de veiligheid ervan niet vertrouwden. Deze indicatie is getoetst met behulp van twee vragen in de enquête:



Figuur 26, "Hebben zorgen over veiligheid u doen afzien van de volgende activiteiten in de afgelopen 6 maanden?"

Bron: TNO enquête Veiligheid en Vertrouwen in ICT 2012 (N= 1042)



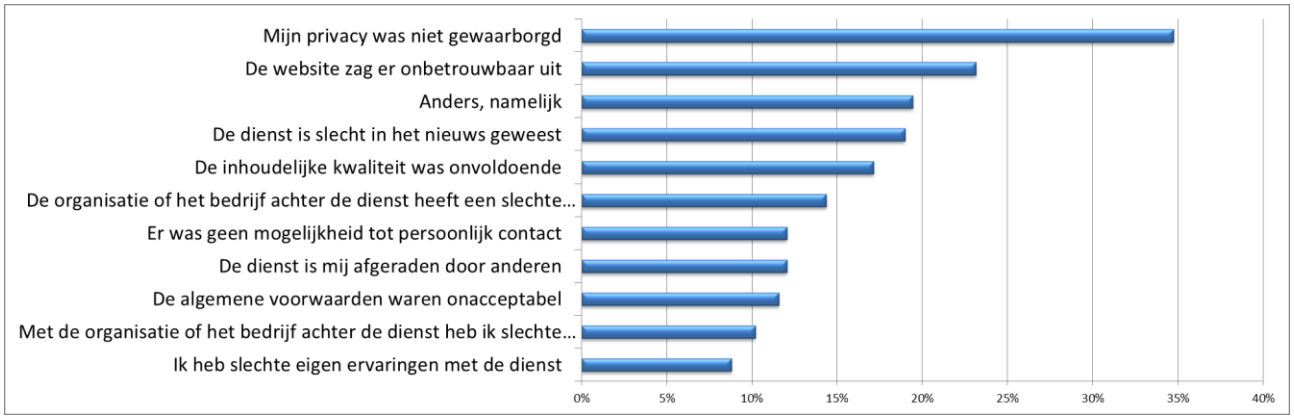
Figuur 27, "Heeft u in de afgelopen 6 maanden een van de onderstaande diensten niet gebruikt omdat u de veiligheid van de dienst niet vertrouwde?"

Bron: TNO enquête Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

Een eerste inzicht uit deze antwoorden is dat burgers blijkbaar een relatief hoog vertrouwen hebben in de veiligheid van de infrastructuur, zoals het vaste en mobiele internet, en telefonie. Maar weinig personen laten het na om deze diensten te gebruiken omdat ze de veiligheid niet vertrouwen.

Ondanks het feit dat banken veel moeite doen om internetbankieren veilig te maken, en de veiligheid hiervan onder de aandacht te brengen, zegt een groep burgers (iets minder dan 10% als we het gemiddelde nemen van beide vragen) desondanks dat ze internetbankieren niet gebruiken omdat ze de veiligheid ervan niet vertrouwen. De omvang van deze groep komt in de buurt van de groep die zegt sociale netwerksites of online winkelen niet te doen wegens zorgen om de veiligheid.

Ook is gevraagd *waarom* burgers die een dienst niet gebruikt de dienst niet vertrouwden:



Figuur 28, "Waarom vertrouwde u deze dienst(en) niet?"

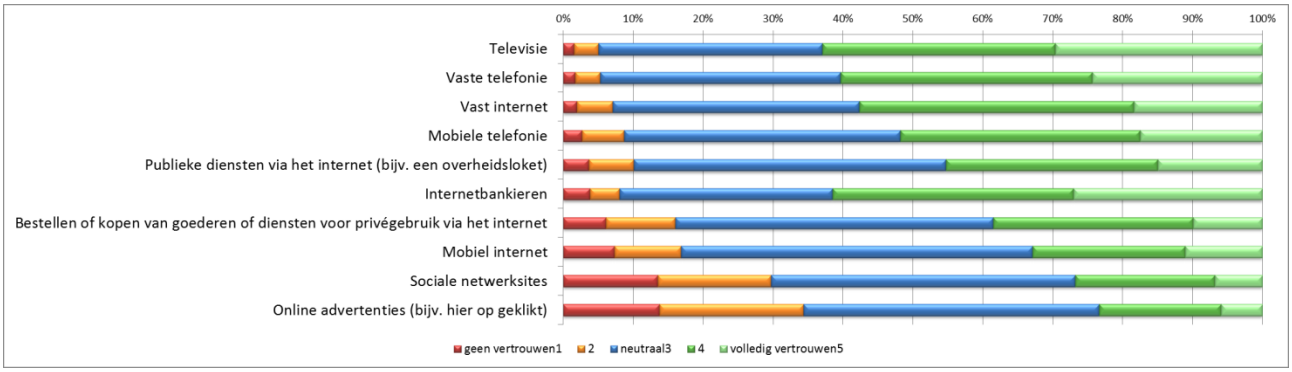
Bron: TNO enquête Veiligheid en Vertrouwen in ICT 2012 (N = 216)

Een echte uitschieter hier is privacy. Van de personen die afzien van het gebruik van (een van de eerder genoemde diensten) geeft maar liefst 35% als reden aan dat de privacy niet gewaarborgd was. Andere, hiermee samenhangende redenen, die vaak genoemd worden zijn de visuele aspecten van de website en dat een dienst slecht in het nieuws geweest is. Slechte eigen ervaringen blijken het minst vaak een rol te spelen. Het blijkt dat een groot deel van de Nederlanders zich wel bewust is van privacy risico's, en om deze reden sommige activiteiten ook daadwerkelijk nalaat om te doen (dit kan bijvoorbeeld dus ook het klikken op een advertentie zijn).

Overigens blijkt het voor respondenten niet altijd makkelijk om de precieze reden voor het gebrek aan vertrouwen onder woorden te brengen. Onder de antwoordcategorie “anders” wordt dit zichtbaar in antwoorden zoals “geen goed gevoel over”, “gevoel”, “ik weet het zelf niet waarom niet”, of “je hoort zoveel, het is een gevoel”.

4.4 Kenmerken organisatie achter ICT

Aan alle respondenten van de TNO enquête is gevraagd naar de mate waarin ze de organisaties achter diensten vertrouwen:



Figuur 29, “Hoeveel vertrouwen heeft u dat aanbieders van de volgende ICT diensten uw veiligheid belangrijk vinden en beschermen?”

Bron: TNO enquête Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

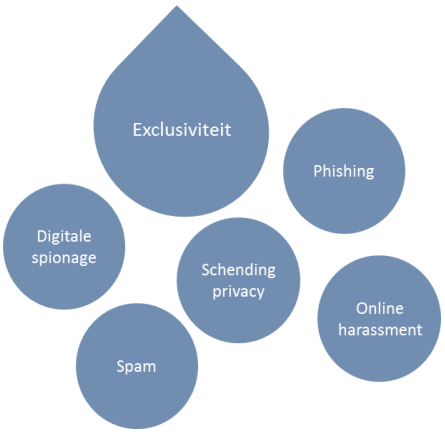
Hier geven de respondenten aan dat de aanbieders van de vaste ICT infrastructuur een vrij hoog vertrouwen genieten, waar banken en de overheid dicht op volgen. Een opvallende negatieve uitschieter is het vertrouwen in de aanbieders van mobiel internet. Wat hierbij een storende factor kan zijn geweest is de mogelijkheid dat respondenten mobiel internet verwarren met bijvoorbeeld de betrouwbaarheid van apps op een mobiele telefoon die van mobiel internet gebruik maken. De respondenten lijken er relatief weinig vertrouwen in te hebben dat aanbieders van sociale netwerksites of marketingpartijen het beste voor hebben met hun veiligheid.

Waar we eerder zagen dat een relatief grote groep (relatief omdat het hier om iets minder dan 10% gaat) respondenten zegt afgezien te hebben van het gebruik van internetbankieren, laat deze antwoorden zien dat banken juist wel goed scoren als het gaat om het vertrouwen van burgers in de mate waarin de veiligheid van hun klanten belangrijk vinden en beschermen.

5 Veiligheid van ICT

In dit hoofdstuk zal voorhanden data ten aanzien van de indicatoren rond exclusiviteit, integriteit en beschikbaarheid behandeld worden. Daarnaast wordt er ook in algemene zin naar cybercrime (niet specfiek voor exclusiviteit, integriteit of beschikbaarheid) gekeken in de laatste sectie.

5.1 Exclusiviteit

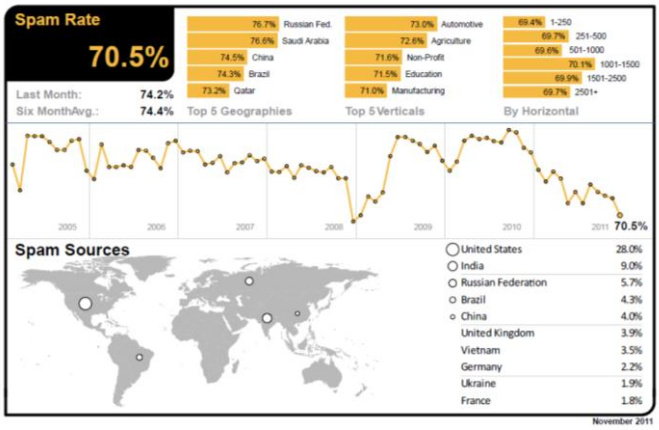


In deze paragraaf worden beschikbare cijfers ten aanzien van 'exclusiviteit' (mate van bescherming van gevoelige informatie tegen onbevoegd en ongeautoriseerd gebruik) gegeven. Hieronder vallen naast de bescherming van systemen tegen digitale spionage ook verschillende vormen van privacy onder. Vaak wordt "lastig gevallen worden" ook onder privacy geschaard; hier hebben we privacy als incorrecte omgang met persoonsgegevens ("Schending privacy"), en lastig gevallen worden (Spam en online harassment) uit elkaar gehaald.

5.1.1 Spam

Betrouwbare emperische informatie over het volume en de financiele consequenties van Spam is moelijk te verkrijgen (zie bijvoorbeeld Robinson, et al. 2012:47). Data die voorhanden zijn worden voornamelijk gegenereerd door bedrijven die beveiligingssoftware ontwikkelen. Deze bedrijven kunnen een prikkel hebben om beveiligingsproblemen te overschatten (zie ook ITU, 2008). Hoewel er inconsistenties zijn in de data geleverd door bedrijven over de hoeveelheid Spam, geven verschillende bedrijven aan dat zij in 2011 een afname van Spam hebben gemeten. MessageLabs Intelligence, onderdeel van het bedrijf Symatec, registreerde de volgende Spam volumes van 2005 tot 2011[9].

[9] Symantec is een bedrijf dat beveiligingssoftware levert. Symatec verzamelt haar data met behulp van het Symantec Global Intelligence Network (ongeveer 240.000 sensors monitoren 'attack' activiteiten via Symantec producten geïnstalleerd bij klanten) en door het verzamelen van 'malicious code intelligence' via producten van ongeveer 133 miljoen client-, server- en gatewaysystemen.



Figuur 30, Gemeten Spam volume 2005 tot en met 2011, Bron: Symantec

Ook het Security Lab van het bedrijf M86 Security laat in hun Spam Volume Index een afname van het Spam volume in 2011 zien[10]. Hoewel de piek- en dalmomenten gemeten door verschillende bedrijven verschillen (M86 Security registreerde in augustus 2011 een dal en Symantec een gemiddeld tot hoog Spam niveau), laten de onderzochte bedrijven een afname van Spam in 2011 ten opzichte van 2010 zien. De voorhanden data beziend, lijkt het Spam volume eind 2011 historisch laag te zijn. In Nederland was in 2011 ongeveer 70 procent van alle email-verkeer Spam.

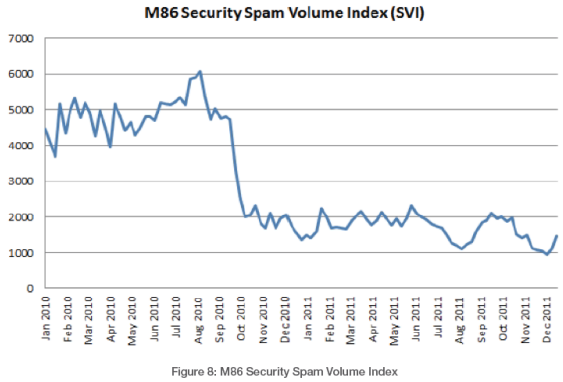


Figure 8: M86 Security Spam Volume Index

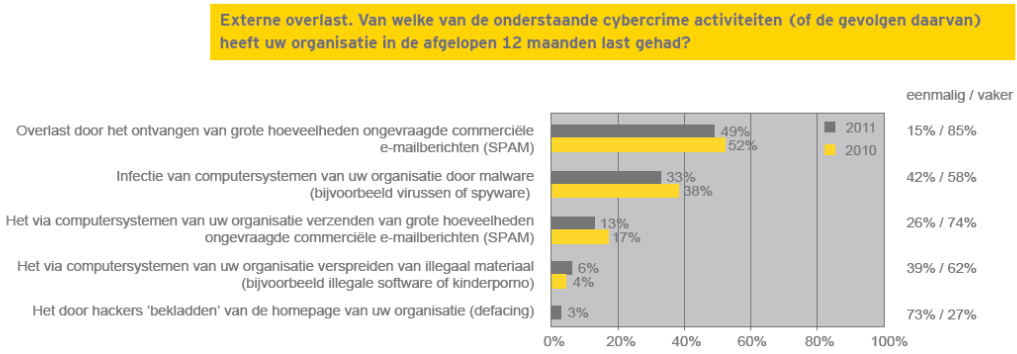
Figuur 31, Gemeten Spam volume 2010-2011, Bron: M86 Security

Het is mogelijk dat het Spam volume in 2011 afnam vanwege effectieve bestreiding van botnets door poltie en justitie uit verschillende landen. In 2011 werd het Rustock botnet afgesloten[11] wat verantwoordelijk was voor het versturen van ongeveer 30 miljoen Spamberichten per dag. In 2010 werden er acties uitgevoerd om de Waledec en BredoLab botnets uit te schakelen. Het Waledac botnet was verantwoordelijk voor ongeveer 1.5 miljard Spam berichten per dag en het BredoLab botnet voor op 3.6 miljard berichten per dag. Zowel BredoLab en Waledac lijken nog steeds gedeeltelijk intact.

[10] M86 Security Lab is eveneens een ontwikkelaar van beveiligingssoftware. M86 Security Lab meet Spam volumes bij klanten die haar producten hebben toegepast. Het is niet duidelijk bij hoeveel klanten M86 Security Lab Spam volumes meet.

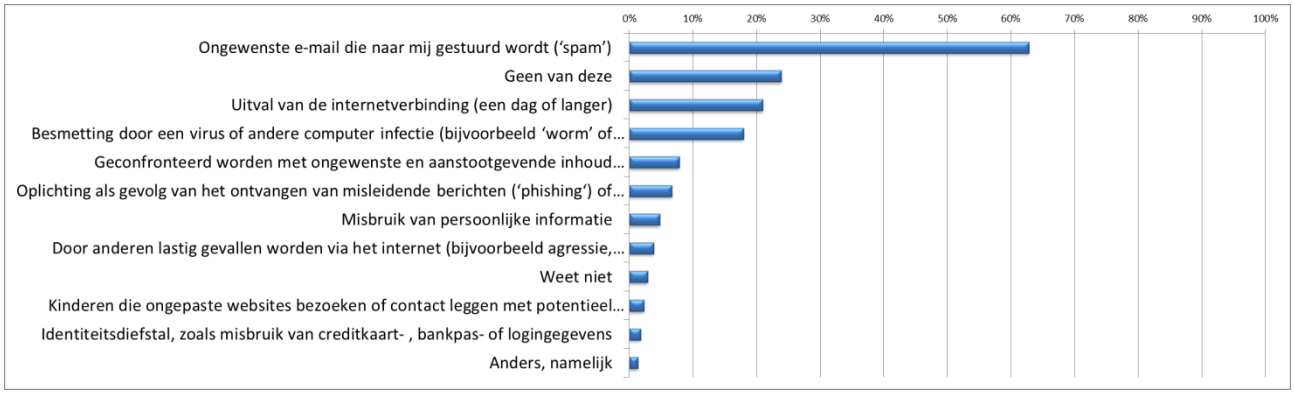
[11] De Amerikaanse politie heeft servers in beslag genomen bij vijf hostingproviders in zeven steden: Kansas City, Scranton, Denver, Dallas, Chicago, Seattle en Columbus. Daarnaast zijn de IP-adressen van degenen die het botnet bestuurden afgesloten.

Dat Spam mogelijk nog steeds de grootste overlast bezorgd bij gebruikers laat de ICT Barometer over Cybercrime van Ernst & Young zien (2011:11). De geenquêteerde bedrijven geven aan dat zij vooral overlast ervaren door Spam.



Figuur 32, Percentage respondenten dat aangeeft in 2011 last te hebben gehad van o.a. Spam, Bron: Ernst & Young

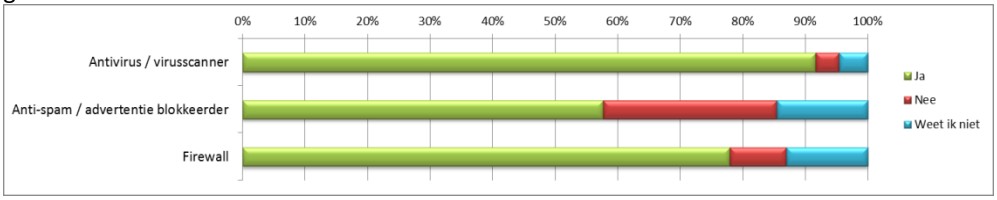
Dit beeld lijkt te worden bevestigd door de TNO enquête uitgevoerd voor dit onderzoek, waaruit blijkt dat Nederlanders in de eerste helft van 2012 vooral last hebben gehad van Spam en virussen. De volgende grafiek geeft een overzicht van het percentage respondenten dat in de eerste helft van 2012 te maken had met specifieke vormen van cybercrime.



Figuur 33, "Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?"

Bron: TNO enquete Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

De onderstaande grafiek laat zien dat de overgrote meerderheid van de respondenten wel gebruik maakt van een virusscanner.



Figuur 34, "Welke software gebruikt u om uw computer te beschermen?"

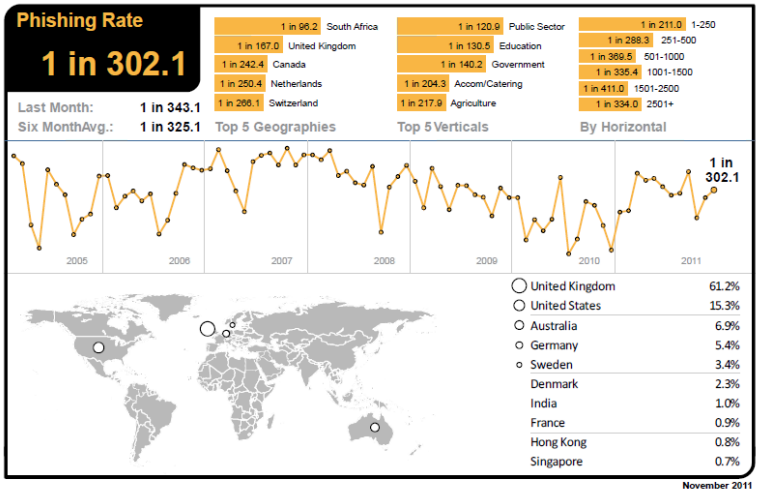
Bron: TNO enquete Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

Daarnaast blijkt uit gegevens van OPTA dat de mondiale afname van Spam in 2011 mogelijk niet doorgewerkt heeft in Nederland. OPTA registreert klachten die via Spamklacht.nl binnenkomen. In 2011 zijn in toaal 27.371 klachten binnengkomen, waarvan de meeste

berichten (24.337) betrekking hadden op Spam via email (OPTA, 2012). Voor email betekent dit een toename van ongeveer 7% ten opzichte van het volume in 2010[12].

5.1.2 *Phishing*

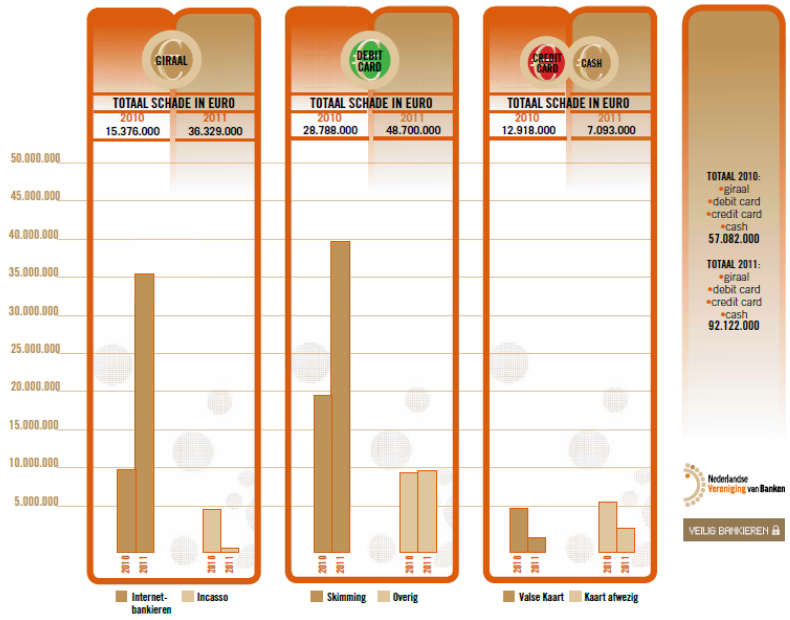
Phishing kan begrepen worden als een poging van een actor om confidentiele informatie van een individu, groep of organisation te verkrijgen via email, instant messaging of een (spoof-)website met als (meest voorkomend) oogmerk financiel gewin. MessageLabs Intelligence, onderdeel van het beveiligingsbedrijf Symatec, registreerde van oktober tot en met november 2011 dat wereldwijd 1 op de 302.1 emails enige vorm van phishing bevatte. Voor Nederland was dit 1 op de 250.4 emails, iets hoger dan het gemeten gemiddelde.



Figuur 35, Gemeten phishing rate 2005 tot en met 2011, Bron: Symantec

Phishing emails worden vaak gebruikt om gebruikers te linken naar een valse bankwebsite (ook wel pharming genoemd) waarop zij hun bankgegevens registreren om vervolgens via internetbankieren geld van de gebruiker te ontvreemden. In deze zin wordt phising door banken vaak gezien als ‘fraude met Internetbankieren’. Onder fraude met Internetbankieren vallen echter ook andere fraudevormen, zoals gevallen waarbij individuen worden gebeld door personen die zich voordoen als bankmedewerkers en trachten bankgegevens te verkijgen. De Nederlandse Vereniging van Banken publiceerde in 2011 het volgende overzicht van geraamde schade als gevolg van fraude met Internetbankieren (waar phising onderdeel van uitmaakt).

[12] Deze toename kan ook veroorzaakt worden doordat meer mensen de website Spamklacht.nl kunnen vinden.



Figuur 36, Raming schade door o.a. fraude met Internetbankieren 2010 en 2011 Bron: DNB

Ten opzichte van 2010 is de schade door fraude met Internetbankieren in 2011 ruim 3 maal zo hoog (9,8 miljoen in 2010 en 36,3 miljoen in 2011). In 2011 zijn er in totaal 7.584 schadegevallen geweest. De Nederlandse Bank meldde in mei 2012 (Rapportage Maatschappelijk Overleg Betalingsverkeer) dat de schade in het Nederlandse betalingsverkeer als gevolg van fraude (waaronder ook niet ICT-gerelateerde fraude) in 2011 in totaal 92 miljoen was. De twee belangrijkste trends die DNB zag, waren de stijgingen als gevolg van fraude bij het internetbankieren en skimming (het kopieren van de magneetstrip van de betaalpas en afkijken pincode). In welke mate fraude met internetbankieren gebeurt door phishing of met behulp van andere methodieken is onduidelijk. Verschillende banken lijken verschillende definities te gebruiken. Onderstaande tabel uit het rapport van PWC (2011:26) geeft de financiële schade voor één grootbank als gevolg van identiteitsfraude in 2010 en de eerste twee maanden van 2011[13]. Hier wordt phishing als identiteitsfraude gezien en als afzonderlijke kostenpost meegenomen.

[13] De bank rapporteerde niet over gevallen van skimming en aan identiteitsfraude te relateren creditcardfraude.

Tabel 2. Frequentie identiteitsfraude

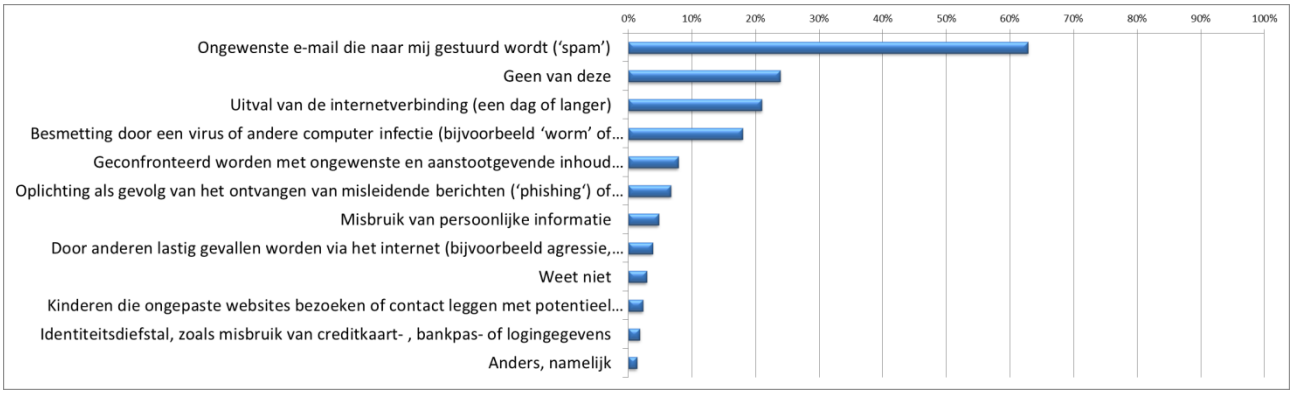
Jaar	Type	Aantal ID-fraude	Schade (€)
2011	Telefonische spoedoverboeking	3	98.778
2011	Phishing	8	85.000
2011	Informatiediefstal / Free format	6	0
2011	Internetbankieren toegevoegd	1	244.994
2011	Frauduleuze aanvraag debitcards	2	9.000
Totaal 2011		**20**	437.772
2010	Phishing	69	436.405
2010	Opheffen en overboeken naar andere bankrekening	3	3.148
2010	Informatiediefstal / Free format	24	69.500
2010	Internetbankieren toegevoegd	12	1.288.776
2010	Frauduleuze aanvraag debitcards	69	2.523.564
Totaal 2010		177	4.321.393

Tabel 3, Frequentie identiteitsfraude van een grootbank in 2010 en eerste twee maanden van 2011, Bron: PWC

In haar ICT Barometer over Cybercrime, presenteert Ernst & Young (2011:12) een figuur met percentages respondenten (vertegenwoordigers van bedrijven) die in 2011 last hebben gehad van vormen van phishing. Gemiddeld heeft ongeveer 10,3% van de ondervraagden in 2011 (eenmalig of verschillende keren) te maken gehad met phishing.

Figuur 37, Percentage respondenten dat in 2011 te maken heeft gehad met verschillende vormen van phishing, Bron: Ernst & Young

De onderstaande grafiek gebaseerd op de TNO enquête uitgevoerd voor dit onderzoek laat zien dat in de eerste helft van 2012 7% van de respondenten aangeeft te maken hebben gehad met oplichting door phishing of spoofing (door worden gestuurd naar nep websites, vaak in combinatie met phishing).



Figuur 38, "Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?"

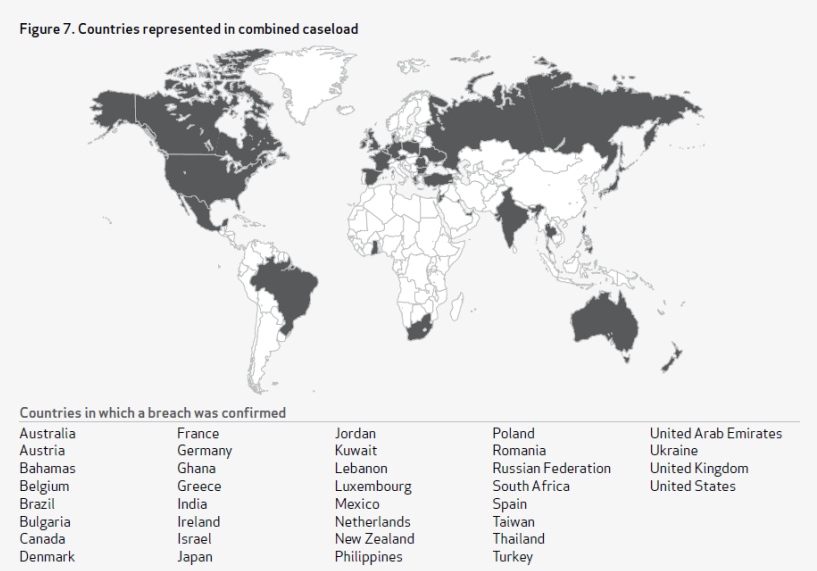
Bron: TNO enquete Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

5.1.3 Privacy schending

Een van de meest voorkomende vormen van privacyschending waarbij ICT een rol speelt zijn 'datalekken' (soms wordt de term datadiefstal gebezigd). Een datalek is het opzettelijk of onopzettelijk vrijkomen van vertrouwelijke informatie in een onbetrouwbare omgeving. Een definitie die door verschillende experts wordt toegepast: "A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so." In april 2011 werd bijvoorbeeld ingebroken op het Playstation Network van Sony waarbij de informatie van ongeveer 100 miljoen gebruikers in handen kwam van derden.

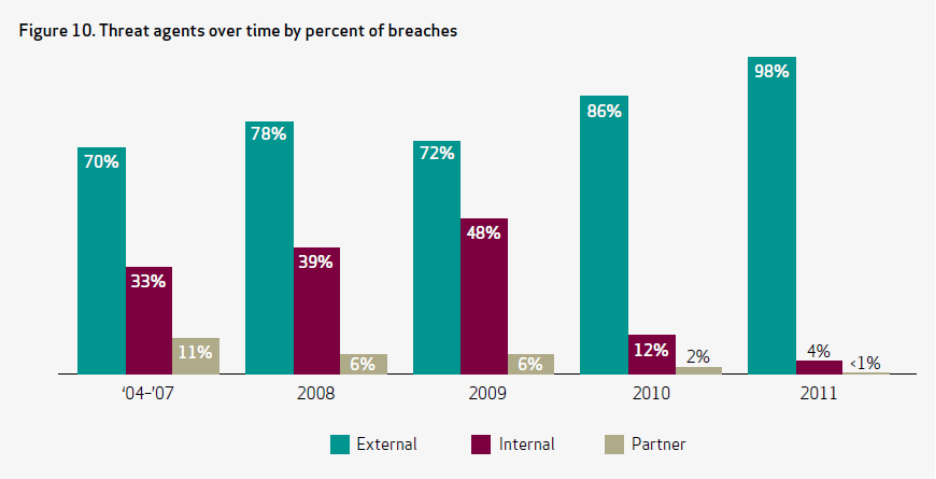
Verizon, een bedrijf dat netwerken, systemen en mobiele technologieën ontwerpt en bouwt, brengt jaarlijks het 'Data Breach Investigations Report' uit. Verizon verzamelt data over voorvallen van data breaches door betaald extern forensisch onderzoek. Het onderzoek wordt geleid door het Verizon RISK Team en data worden aangeleverd door Australian Federal Police, Dutch National High Tech Crime Unit, Irisch Reporting & Information Security Service, Scotland's Police Sentral e-Crime Unit, en United-States Secret Service. Deze organisaties gezamenlijk meldden in 2011 855 voorvallen van datalekken en rond de 174 miljoen vrijgekomen records. Verizon geeft in haar rapport aan dat de genomen sample niet representatief is voor alle data breaches wereldwijd. Omdat Verizon geen inzicht heeft in het totale aantal data breaches wereldwijd kan zij de representativiteit en precieze foutmarge niet berekenen.

Hoewel Verizon geen inzicht geeft in aantallen data breaches per land, geeft zij wel aan in welke landen tenminste één data breach heeft plaatsgevonden.



Figuur 39, Landen waarin ten minste 1 voorval van data breach is gevonden, Bron: Verizon

Daarnaast heeft Verizon de afgelopen jaren bijgehouden welk type 'agent' (dader) de data breach heeft veroorzaakt en maakt hierbij onderscheid tussen een externe, interne of partner dader. In de datasets van Verizon is over de jaren het aantal externe daders toegenomen (zie Figuur 40)[14].

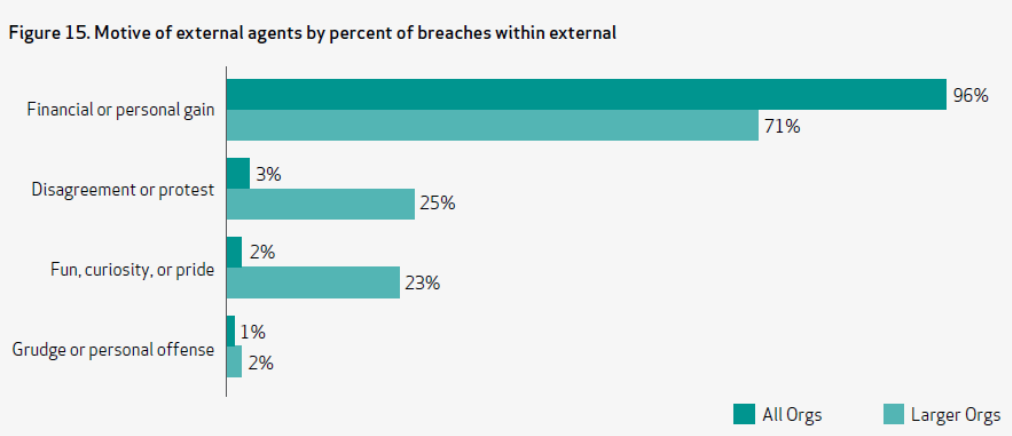


Figuur 40, Percentage data breaches per agent, Bron: Verizon

Verizon verklaart de toename van externe daders doordat externe daders vaak op een groter aantal slachtoffers doelen dan interne daders, wat het beeld kan vervormen wanneer wordt gekeken vanuit aantallen slachtoffers (in plaats van aantallen daders). Een andere verklaring is het feit dat in 2011 een groot aantal hack-incidenten kende, wat per definitie door externen plaatsvindt.

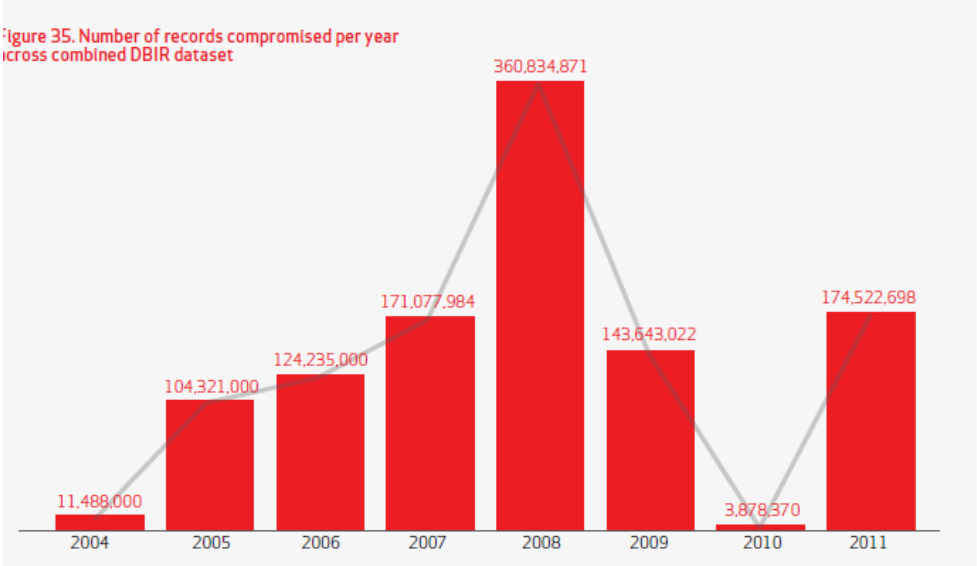
Daarnaast was in 2011 het belangrijkste motief om over te gaan tot het plegen van data breaches financiële of persoonlijk gewin (zie Figuur 41). Hier zit volgens Verizon geen significant verschil met voorgaande jaren.

[14] NB: Geen consistente sample; de eerste jaren waren gebaseerd op cases alleen verzameld door Verizon. In latere jaren participeerden organisaties zoals United-States Secret Service.



Figuur 41, Percentage agents per motief om tot data breach over te gaan, Bron: Verizon

Verizon laat het volgende overzicht zien van gestolen records in de jaren 2004 tot en met 2011. In 2011 vond Verizon het een na hoogste aantal lekken van records.



Figuur 42, Aantallen gelekte records in de jaren 2004-2011, Bron: Verizon

Het relatief lage aantal gestolen records in 2010 verklaart Verizon aan de hand van het type criminelen. Terwijl in 2011 financieel gedreven criminelen tot doel hadden om (geautomatiseerd) grote aantallen records te stelen, leek in 2010 een aantal acties gericht op het verkrijgen van enkele (zeer waardevolle) records.

Wat betreft cijfers in Nederland meldt de ICT Barometer over Cybercrime van Ernst & Young (2011:13) dat 5% van de ondervraagde professionals aangeeft dat hun organisatie de afgelopen 12 maanden last heeft gehad van diefstal van klantgegevens of bedrijfsinformatie via computersystemen. Dit is een afname van 2% ten opzichte van 2010.

Figuur 43, Percentage respondenten dat aangeeft in 2011 last gehad te hebben van o.a. diefstal van gegevens, Bron: Ernst & Young

Het NCSC (2012:23) geeft het volgende overzicht ten aanzien van aantal afgehandelde incidenten in Nederland waarbij gegevens van overheden uitgelekt zijn in 2011 (26) en het eerste kwartaal van 2012 (12).

Tabel 2. Door NCSC afgehandelde incidenten met uitgelekte gegevens

11Q1	11Q2	11Q3	11Q4	12Q1
3	4	11	8	12

Tabel 4, Door NCSC afgehandelde incidenten met uitgelekte gegevens, Bron: NCSC

Cijfers over privacy schendingen worden ook gegeven door het College Bescherming Persoonsgegevens (CBP), welke in 2010 de website www.mijnprivacy.nl lanceerde. Op deze website wordt algemene voorlichting gegeven over het waarborgen van de persoonlijke levenssfeer en kunnen burgers meldingen doen van voorvallen van onzorgvuldige of onrechtmatige verwerking van persoonsgegevens. Sinds het moment dat deze meldingen mogelijk werden gemaakt (april 2011) tot en met december 2011 kwamen via de website in totaal 4.311 signalen binnen. In 2011 zijn in totaal 5790 signalen binnengekomen via de website, het telefonisch spreekuur en per post. De meeste signalen hebben betrekking op de sectoren Handel en Dienstverlening (32,3%), Openbaar Ministerie (16,5) en Arbeid (13,4%), zie Tabel 5.

Toezicht en naleving	Totaal 2011
Andere sector	425
Arbeid	772
Betrokkene	346
Handel & Dienstverlening	1871
Internationale Organisaties	37
Internet	301
Openbaar Bestuur	954
Overige instellingen	17
Politie & Justitie	154
Sociale zekerheid	50
Telecom	149
Zorg & Welzijn	686
Leeg	28
Totaal	**5790**

Figuur 2 Verdeling signalen binnen 'Andere sector'

Belangenorganisatie	84
Cultuur, Sport en Recreatie	127
Klachteninstantie	3
Media	57
Onderzoeks- en researchinstituut	16
Overige	41
Kerkelijke instelling	18
Toezichthouder	79
Totaal	**425**

Binnengekomen signalen vallen onder 'Andere sector' verdeeld naar instanties

Tabel 5, Aantallen meldingen voorvallen privacy schending 2011, Bron: CBP

Bij de categorie Politie en Justitie gaat het vooral om signalen over de politie. Meldingen over internet betreffen vooral zoekmachines en sociale netwerksites (samen 50,8%). Binnen de categorie Telecom gaat het voornamelijk over operators (91,7%). Bij de categorie Sociale Zekerheid betroffen de meldingen zowel het UWV (48,9%) als de sociale dienst (34,6%). De meest voorkomende type melding zijn het verstrekken van gegevens

aan derden, verwerking van gegevens die via het Internet verkregen zijn en heimelijke waarneming (bijvoorbeeld cameratoezicht en tracking & tracing). Het CBP (2011:49) gaf in haar jaarverslag het volgende overzicht per sector.

Per hoofdsector gaan de meeste signalen over de volgende onderwerpen:

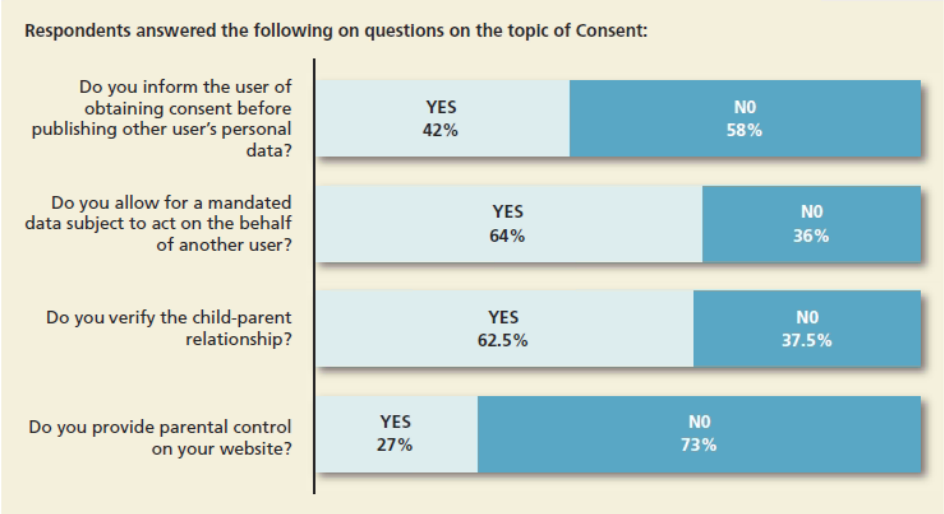
- Handel en Dienstverlening: het verstrekken van persoonsgegevens aan derden, gegevensverwerkingen ten behoeve van identificatie en het gebruik van het burgerservicenummer.
- Openbaar Bestuur: het verstrekken van persoonsgegevens aan derden, heimelijke waarneming al dan niet door cameratoezicht en de publicatie van persoonsgegevens op internet.
- Arbeid: verstrekking van persoonsgegevens aan derden, het gebruik van het burgerservicenummer en personeelsvolgsystemen.
- Politie en Justitie: derdenverstrekking.
- Internet: publicatie persoonsgegevens op internet, beveiliging van persoonsgegevens en datalekken en het verstrekken van persoonsgegevens aan derden.
- Telecom: identificatie en het verstrekken van persoonsgegevens aan derden.
- Sociale zekerheid: verstrekken van persoonsgegevens aan derden.
- Zorg en Welzijn: gegevensverwerkingen met betrekking tot het (medisch)dossier en het verstrekken van persoonsgegevens aan derden.
- Internationale organisaties: doorgifte derde landen en heimelijke waarneming (bestaande uit heimelijke waarneming, heimelijke waarneming – cameratoezicht en heimelijke waarneming – tracking&tracing).

Tabel 6, Type melding per hoofdsector 2011, Bron: CBP

In 2011 voerde Enisa een studie uit naar onder andere privacy mechanismen in online omgevingen. Voor deze studie vulden 18 organisaties die online diensten verstrekken een vragenlijst in, waarvan 11 deelnemers alle vragen beantwoordden en 7 niet alle vragen (Enisa, 2011:11)[15]. Van de 7 organisaties die niet alle vragen hebben beantwoord, waren 3 vragenlijsten voldoende beantwoord (3/4) om deze te kunnen verwerken in het rapport. Enisa wijst op de beperkingen van het onderzoek en geeft aan dat de resultaten indicaties zijn voor verbetering en gebruikt kunnen worden om verder richting te geven aan onderzoek. Op basis van het onderzoek kunnen geen definitieve conclusies worden getrokken over de status van privacy mechanismen in bedrijven.

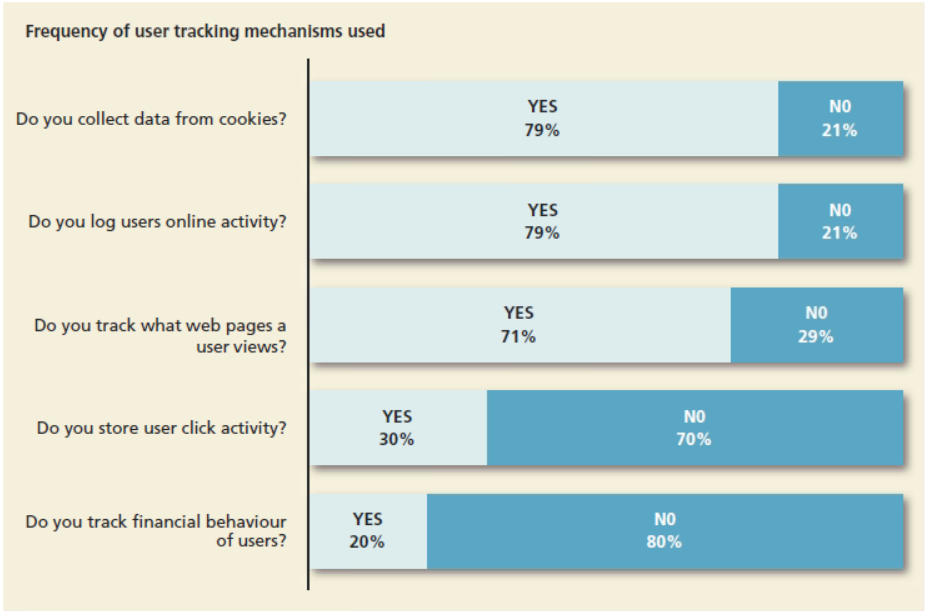
Enisa vroeg de betrokken organisaties naar de mate waarin zij 'user consent' waarborgen (het voorzien in toestemming, overeenstemming, uitgebreid overwegen van mogelijkheden om persoonlijke gegevens vrij te geven of te beschermen). 79% van de ondervraagde organisaties gaf aan dat het voorafgaande aan registratie door gebruikers noodzakelijk is dat gebruikers instemmen met een Term of Use, Service en/of Privacy Policy. 67% gaf aan dat zij regelmatig deze terms en/of policies veranderen en wanneer zij dit veranderen informeert 56% van de ondervraagde organisaties gebruikers hierover. De organisaties als volgt antwoord op de volgende specifieke vragen over consent:

[15] Enisa benaderde 200 organisaties voor deelname, 30 gaven aan deel te willen nemen aan het onderzoek, hiervan hebben 18 organisaties de vragenlijst ingevuld.



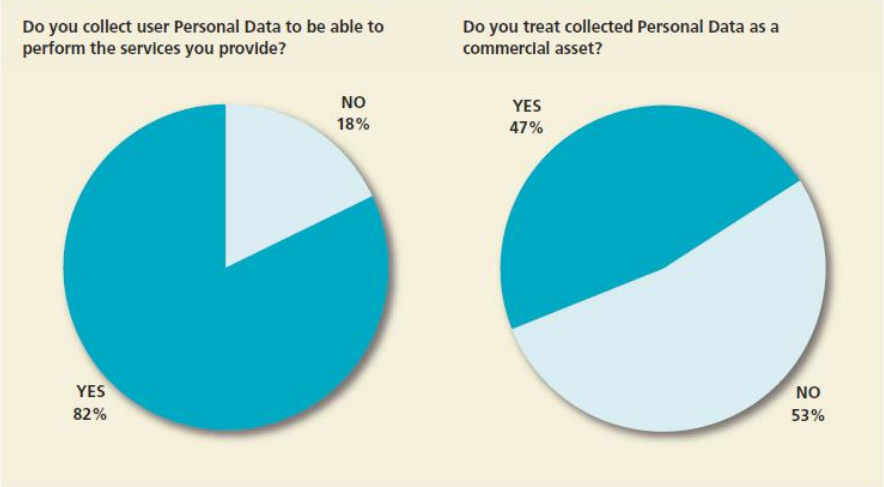
Figuur 44, Percentage respondenten per vraag over consent, Bron: Enisa

Daarnaast stelde Enisa een aantal vragen over het verzamelen van gegevens van gebruikers door betrokken organisaties. Hieruit bleek dat het merendeel van de ondervraagde organisaties gegevens verzamelen via cookies. De organisaties gebruiken cookies om verschillende redenen, zoals het tegengaan van fraude en handhaven van veiligheid en voor marketing (bijv. 'behavioural targeting'). Voorts gaven de ondervraagden als volgt antwoord op de volgende specifieke vragen over tracking mechanismen.

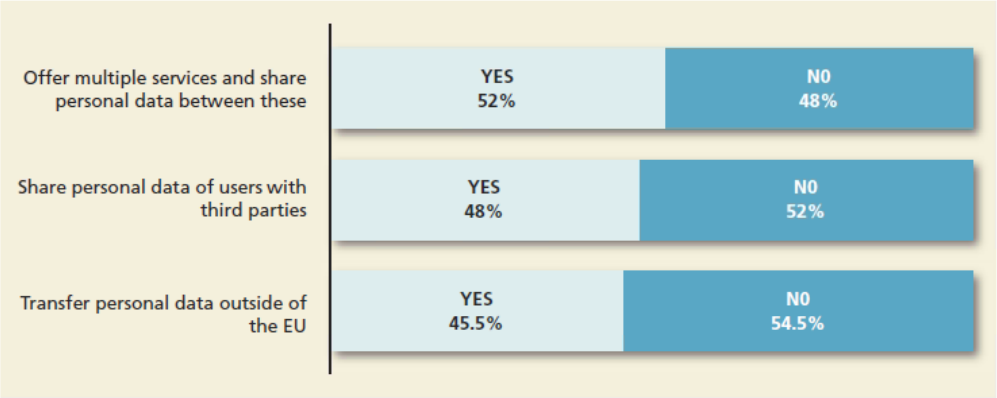


Figuur 45, Percentage respondenten dat user tracking mechanismen gebruikt, Bron: Enisa

Tot slot vroeg Enisa naar de reden waarom organisaties gegevens verzamelden en de mate waarin organisaties gegevens van gebruikers delen met derden. Figuur 46 en 47 geven een overzicht van de survey resultaten.



Figuur 46, Percentage respondenten dat persoonlijke data verzamelt voor het leveren van diensten en voor commercieel gebruik, Bron: Enisa



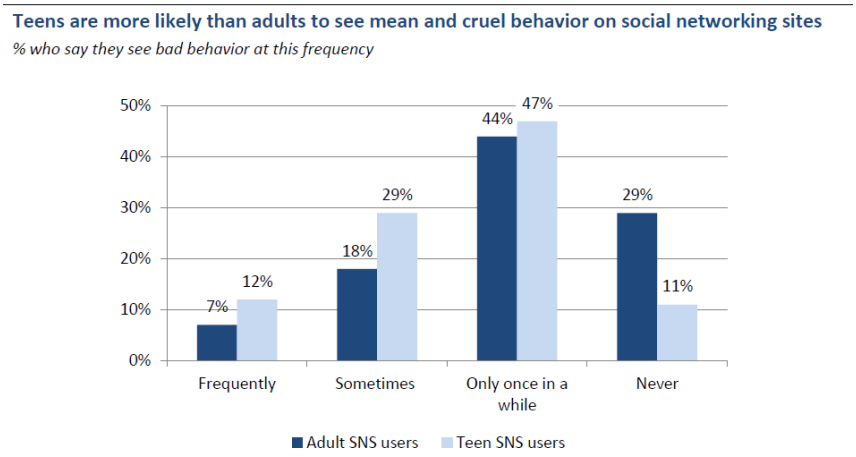
Figuur 47, Percentage respondenten dat persoonlijke data deelt met specifieke partijen, Bron: Enisa

De resultaten van het onderzoek van Enisa overziend, lijkt het voor eindgebruikers in geval van de ondervraagde bedrijven niet altijd goed in te schatten in welke mate hun persoonlijke gegevens beschermd zijn tegen (commercieel) gebruik door partijen. Hoewel het merendeel van de organisaties een Terms of Use en/of Privacy policy heeft, laat ongeveer de helft de gebruiker weten wanneer beleid wijzigt. Opvallend is ook dat geen van de bedrijven positief antwoordde op de vraag of gebruikers bij het opstellen van een privacy beleid betrokken worden. De vraag blijft of en in welke mate eindgebruikers invloed kunnen uitoefenen op het gevoerde privacy beleid, c.q. keuzes hebben ten aanzien van de bescherming van hun persoonlijke data.

5.1.4 Online harassment

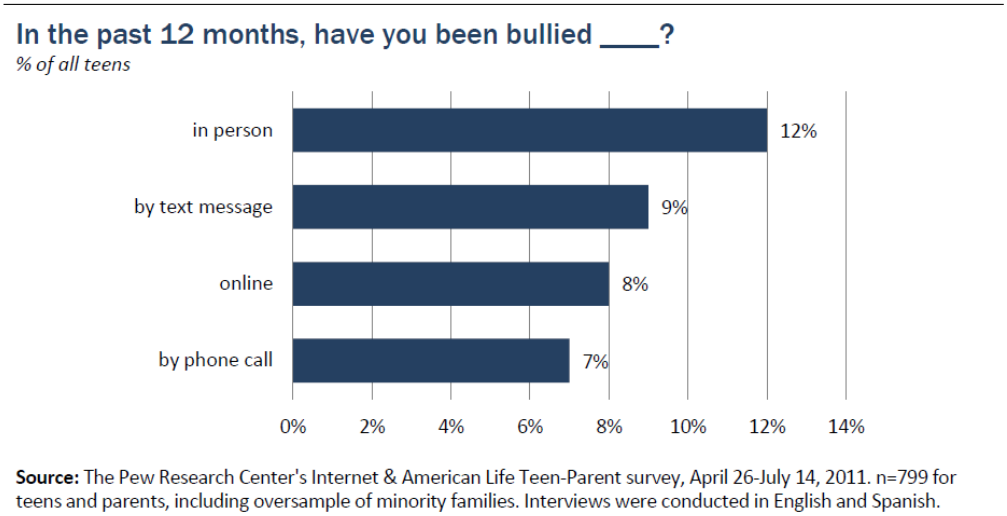
Onder online harassment kan worden verstaan het gebruik van ICT (bijv. Internet, emails of SMS) om anderen te kwetsen door bijvoorbeeld bedreiging, stalken, pesten of seksuele intimidatie. Omdat het een breed begrip betreft zijn er voornamelijk studies over specifieke vormen van online harassment. Studies met actuele cijfers over vormen van online harassment in Nederland zijn echter schaars. Pew Research Center (2012) deed onderzoek in de Verenigde-Staten naar de vriendelijkheid van interacties op social networking sites en bracht daarbij 'mean and cruel' gedrag bij in kaart. Zij voerde in 2011 een survey uit onder 1.716 volwassenen en 799 tieners (leeftijd 12-17) en ouders. Op de

vraag in hoeverre ondervraagden gemeen gedrag tegen kwamen, werd door 29% van de volwassenen en 7% tieners nooit geantwoord (zie Figuur 48). 69% van de volwassenen en 88% van de tieners kwam er wel mee in aanraking.



Figuur 48, Percentage ondervraagden dat in aanraking kwam met onaardig of gemeen gedrag op social networking sites, Bron: PEW Research Center

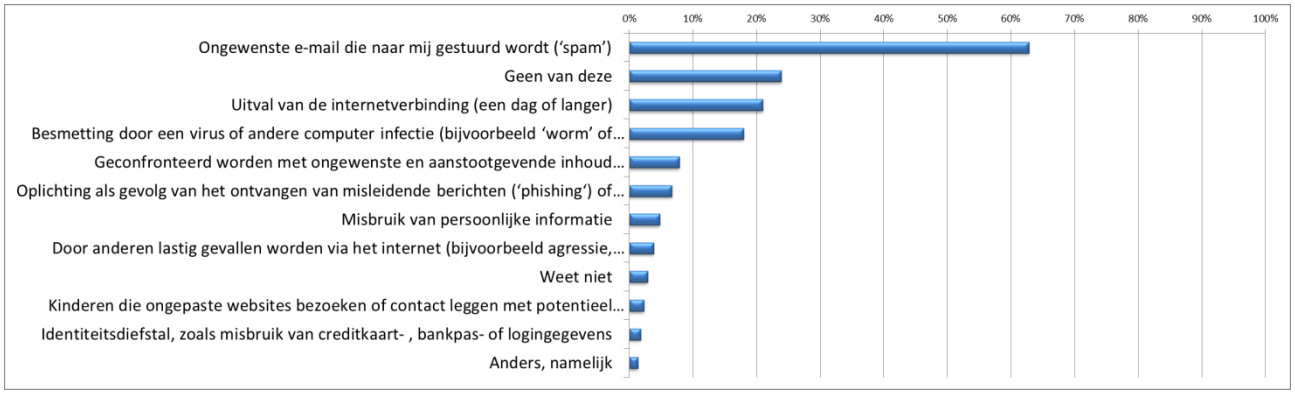
Het bleek dat de ondevraagde tieners significant vaker dan volwassenen in aanraking kwamen met onaardig of gemeen gedrag van anderen. In een aanvullend onderzoek van Pew Research Center (2011) dat specifiek ingaat op het gedrag van tieners op social networking sites werden tieners en ouders gevraagd of zij de afgelopen 12 maanden via social networking sites gepest zijn. Hieruit bleek dat gemiddeld 9% van de ondervraagde tieners in de afgelopen 12 maanden was gepest via verschillende media.



Figuur 49, Percentage ondervraagden dat in 2011 was gepest via verschillende media, Bron: PEW Research Center

Wat betreft cijfers over online harassment in Nederland is de Meldknop.nl relevant, welke begin 2012 is ingesteld door Digibewust (Digibewust is een programma belegd bij bij het Electronic Commerce Platform Nederland). De Meldknop.nl is een website voor jongeren tussen 11 en 16 jaar die informatie, hulp en advies biedt wanneer ze te maken hebben met vormen van online harassment. Kinderen en jongeren kunnen via de website melding hiervan maken. De cijfers over meldingen van online harassment zijn echter niet beschikbaar gesteld aan TNO voor onderzoek. Mogelijk dat deze cijfers in een volgende monitor wel meegenomen kunnen worden.

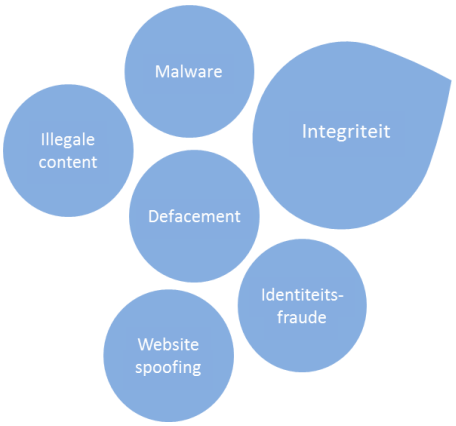
Tot geeft de TNO enquête die is uitgevoerd voor dit onderzoek een indicatie van de mate waarin online harassment in Nederland voorkomt. Onderstaande grafiek laat zien dat 4% van de respondenten aangaf in de eerste helft van 2012 te maken hebben gehad met een vorm van online harassment.



Figuur 50, "Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?"

Bron: TNO enquete Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

5.2 Integriteit



In deze paragraaf worden beschikbare cijfers ten aanzien van 'integriteit' (rond het correct en volledig zijn van informatie en software) gepresenteerd. De integriteit van software en informatie wordt in de praktijk op verschillende manieren geschonden: middels kwaadaardige software (malware), het hacken van websites ("defacement"), en andere manieren. We scharen hier ook illegale content onder, wat niet direct met integriteit te maken heeft, omdat deze hier inhoudelijk wel beter past dan bij exlusiviteit of beschikbaarheid.

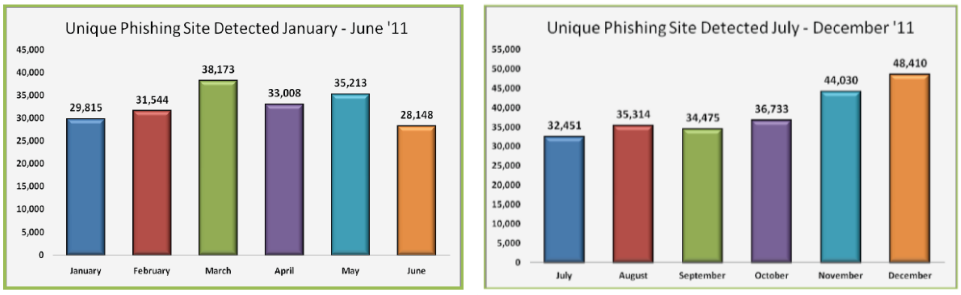
5.2.1 *Website Spoofing*

Bij website spoofing wordt een website gecreerd met als intentie om het aan gebruikers te doen voorkomen dat de website door een andere persoon of organisatie is gecreëerd. Vaak wordt in de website het design van een organisatie overgenomen of wordt een website totaal nagebouwd. Soms heeft de spoofwebsite dezelfde URL als de website van de organisatie die doelwit is van de actie. Spoofwebsites worden vaak ingezet in combinatie met phishing emails. Een gebruiker krijgt een email via welke hij/zij naar een nagebouwde website wordt geleid (bijv. van een bank) en gevraagd wordt om bepaalde gegevens te registreren. Deze gegevens worden vervolgens gebruikt voor criminele activiteiten.

Spoofwebsites worden vaak phishing sites genoemd, omdat de meest voorkomende vorm van spoofwebsites webpagina's zijn waar om persoonlijke gegevens wordt gevraagd. Het begrip spoofwebsite is echter breder, hier vallen ook namaakt pagina's onder waarop onjuiste of schadelijke berichten voor een organisatie of persoon worden gepubliceerd[16]. Hoewel er weinig data zijn over aantallen spoofwebsites, rapporteert the Anti-Phishing Working Group (APWG) jaarlijks cijfers over aantallen phishing websites[17]. Op de website van APWG kunnen voorvallen van o.a. phishing sites worden gemeld. Over 2011 rapporteerde APWG de volgende aantallen phishing websites.

[16] Zo werden in 2006 twee spoof websites gecreëerd, www.msfirefox.com en www.msfirefox.net waarop gesteld werd dat Microsoft Firefox had gekocht.

[17] 'The APWG, established in 2003 as the Anti-Phishing Working Group, is an industry association focused on unifying the global response to cybercrime. The organization provides a forum for responders and managers of cybercrime to discuss phishing and cybercrime issues, to consider potential technology solutions, to access data logistics resources for cybersecurity applications and for cybercrime forensics, to cultivate the university research community dedicated to cybercrime and to advise government, industry, law enforcement and treaty organizations on the nature of cybercrime.'



Figuur 51, Unieke phishing sites gedetecteerd tussen januari en december 2011, Bron: APWG

APWG meldt dat er in 2011 een zichtbare trend was van phishers om in plaats van een URL met de naam van een organisatie erin te gebruiken te hosten op een 'compromised domain'. 16% minder vaak werd een URL gebruikt met daarin de naam van de organisatie die doelwit was. Het lijkt erop dat phishers hun strategie wijzigen omdat meer mensen op de hoogte zijn van kenmerken van phishing websites.

Cijfers over phishing sites in Nederland worden gegeven in de ICT Barometer over Cybercrime van Ernst & Young (2011:12). Ernst & Young meldt dat 10% van de door hun ondervraagde professionals van bedrijven in 2011 last had van phishing websites (zie Figuur 52 hieronder) [18]. De unit "IT Risk and Assurance" van Ernst & Young Nederland publiceert een jaarlijkse rapportage waarin zij een beeld schetsen van de mate waarin bedrijven te maken zouden hebben met voorvallen van Cybercrime[19].

Figuur 52, Percentage respondenten dat meldt last te hebben gehad van phishing activiteiten in 2011, Bron: Ernst & Young

5.2.2 *Identiteitsfraude*

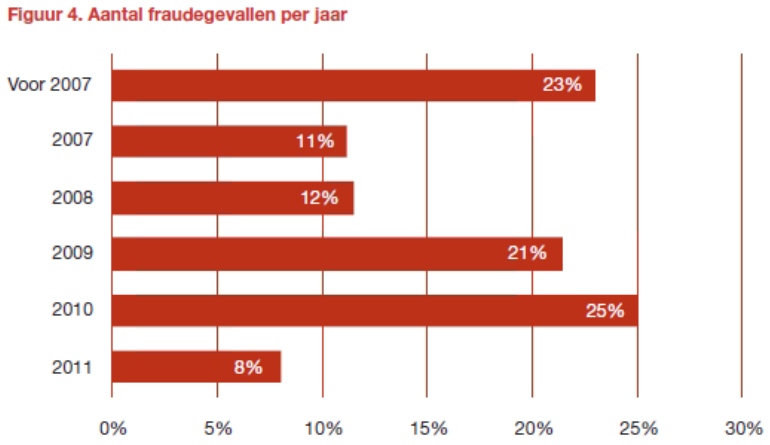
Gerelateerd aan phishing, maar een bredere categorie van criminaliteit, is identiteitsdiefstal. Identiteitsdiefstal bestaat uit het aannemen van de identiteit van een ander (levende of overleden, bestaande of fictieve) persoon met als doel om daaruit voordeel te behalen (Garlik, 2009). Identiteitsdiefstal is sterk gerelateerd aan ICT omdat het vaak gepaard gaat met het gebruik van (veelal digitaal opgeslagen) persoonlijke gegevens van derden. Phishing kan worden gezien als een methodiek om aan (o.a.) identiteitsgegevens te komen. Een andere methodieken om aan identiteitsgegevens te komen is bijvoorbeeld harvesting (het afschuimen van sociale websites op zoek naar

[18] Ernst&Young geeft in haar verantwoording (2011:30) aan dat de cijfers gebaseerd zijn op vragen gesteld aan gemiddeld 600 Nederlandse directeuren, managers of professionals uit het bedrijfsleven, verdeeld over 4 sector (productie/industrie, handel/distributie, dienstverlening/financiële instellingen en (semi)overheid) en bedrijfsgrootte. Verder geeft Ernst & Young in een reactie aan dat de steekproef is genomen uit een online panel met stratificatie naar leeftijd, geslacht, opleiding en branche. De vragenlijst bevatte gesloten vragen met bij elke vraag een 'weet niet' optie. Een groep van ongeveer 25% was niet in staat om alle vragen te beantwoorden. De sample lijkt krap, maar kan bij goede spreiding (demografisch en naar sector) voldoende zijn.

[19] Cijfers gegenereerd door een bedrijf dat adviseert op het gebied van Cybersecurity kunnen beperkt objectief zijn omdat zij mogelijk een prikkel hebben om Cybercrime te overschatten.

persoonlijke informatie). Identiteiten worden door derden veelal gebruikt voor financieel gewin (bijv. verzezekeringsfraude, creditcard fraude), het begaan van overtredingen en misdrijven (bijv. verpreiding illegale content of online harassment) of het verkrijgen van rechten (denk aan sociale zekerheidsrechten). Identiteitsfraude kan gepleegd worden door het overnemen van een bestaande identiteit of door het creëren en aannemen van een nieuwe identiteit.

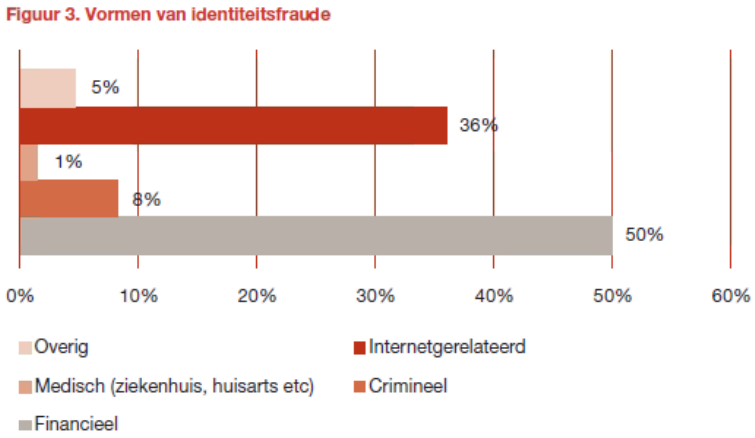
PWC (2011:64) presenteert in haar rapportage over identiteitsdiefstal cijfers uit haar internetenquête onder 5.000 Nederlandse burgers. In deze enquete antwoordden 280 van de 5000 respondenten (5,6%) dat zij ooit te maken hebben gehad met identiteitsdiefstal[20]. Voorts is door PWC aan deze 280 respondenten gevraagd om aan te geven in welk jaar de identiteitsfraude(s) had(den) plaatsgevonden. Deze laatste vraag leverde het beeld uit Figuur 53 op. NB: de cijfers van 2011 waren niet compleet; omdat de enquête in maart 2011 is uitgezet, geven de cijfers van 2011 slechts de eerste twee maanden uit 2011 weer.



Figuur 53, Percentage respondenten dat te maken heeft gehad met identiteitsdiefstal in jaren 2007-2011 (2011 januari en februari), Bron: PWC

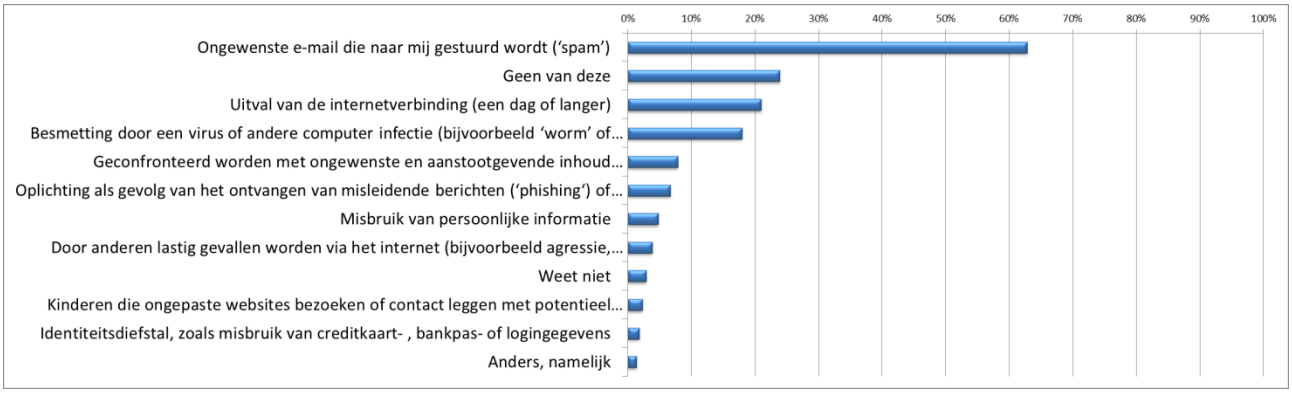
Daarnaast is door PWC aan de 280 van de 5000 respondenten die te maken hebben gehad met identiteitsfraude gevraagd met welke vorm zij te maken hadden waarbij gekozen kon worden tussen internetgerelateerd, medisch, crimineel of overig. 36% van de respondenten gaf aan te maken hebben gehad met internetgerelateerde fraude, waar PWC (2011:68) o.a. onder verstaat: misbruik van persoonsgegevens om op het internet producten aan te schaffen, gebruik van identiteit om een website of e-mailadres aan te vragen, publicatie van een bericht op een site onder andermans naam zonder diens toestemming.

[20] Gegeven de door PWC berekende nauwkeurigheidsmarge betekent dit tussen de 2,98% en 8,22%



Figuur 54, Percentage respondenten dat aangeeft te maken te hebben gehad met een specifieke vorm van identiteitsfraude, Bron: PWC

De onderstaande grafiek gebaseerd op de TNO enquête uitgevoerd voor dit onderzoek laat zien dat 2% van de respondenten aangeeft in de eerste helft van 2012 te maken hebben gehad met identiteitsdiefstal.



Figuur 55, "Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?"

Bron: TNO enquete Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

5.2.3 *Illegale content*

Een andere vorm van cybercrime betreft het produceren, aanbieden, verspreiden en consumeren van illegale content. Het kan hierbij gaan om zeer ernstige misdrijven zoals in geval van kinderporno, maar ook om lichtere delicten zoals het aanbieden van content waarop copyright berust. Wat het laatste betreft houdt Stichting Brein[21] statistieken bij van het aantal Nederlandse sites met illegale bestanden. Over het jaar 2011 meldde stichting Brein dat zij 594 sites hebben gesloten die toegang boden tot illegale content en 14 sites die illegale kopieën op dragers (van informatie; bijvoorbeeld computers) te koop aanboden. Naar schatting werden door interventies van Brein ongeveer 60.000 advertenties voor illegale kopieën op dragers verwijderd. Brein meldt voorts dat de politie 4 inbeslagnames heeft uitgevoerd van in totaal 540 dragers van illegale content. Brein zelf nam 6.377 dragers met illegale content in beslag.

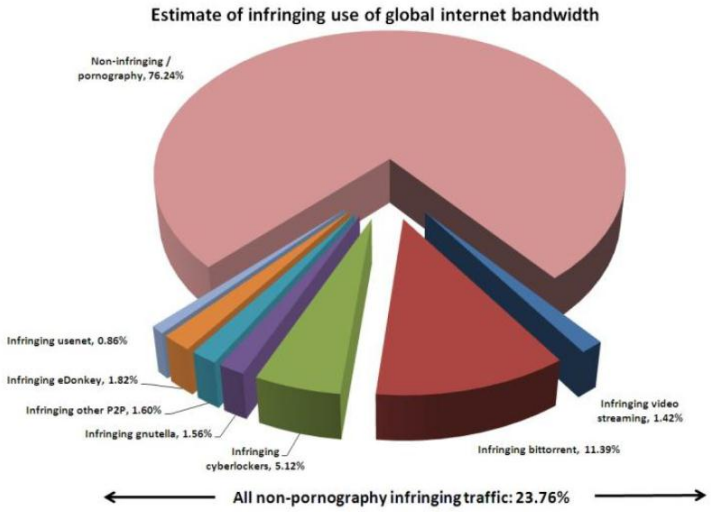
[21] Stichting BREIN is een samenwerking tussen auteurs- en naburig rechthebbenden op het gebied van bescherming tegen ernstige en georganiseerde inbreuk en misbruik van hun werk. Stichting BREIN bestrijdt Intellectueel Eigendomsfraude namens auteurs, uitvoerende kunstenaars, uitgevers, producenten en distributeurs van muziek, film, video, boeken, games en interactieve software.

In 2011 voerde het bedrijf Envisional[22] een onderzoek uit naar de mate waarin illegale content voorkwam op het Internet. Om een inschatting te kunnen maken van de hoeveelheid illegale content maakte Envisional gebruik van de data van een zogenaamde tracker (2011:7). Een tracker is een centrale server welke gebruikers ondersteunt bij het vinden van specifieke files als zij deze middels een gedistribueerd netwerk (peer-to-peer, vaak een "torrent") willen downloaden.

De tracker registreert het IP adres van gebruikers die files verspreiden en delen. Ook registreren trackers de data van elke file die zij vinden op het Internet. Deze data beteffen onder andere de 'hash' van de file (een unieke code waarmee de file herkend kan worden), het aantal seeds (gebruikers die een gehele kopie hebben van de file), de leechers (gebruikers die downloaden) en totaal aantal volledige downloads.

Envisional analyseerde de data van de tracker PublicBT Tracker, welke op het moment van het onderzoek data van ruim 2.7 miljoen individual torrents bevatte. De data van ruim 2.7 miljoen individual torrents is gebruikt om een schatting te maken van het volume van illegale content aanwezig op het Internet.

Envisional kwam op basis van de data tot de inschatting dat 23,76% van het Internetverkeer illegaal was (2011:2). Hierbij werd pornografie als niet strafbaar begrepen.



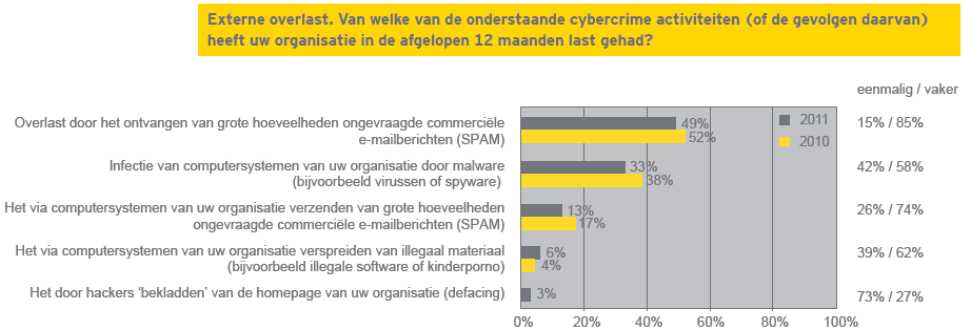
Figuur 56, Inschatting illegale content wereldwijd 2011 – pornografie als niet illegaal begrepen, Bron: Envisional

De mate van illegaal verkeer varieerde per 'internet venue' en was het hoogst in die domeinen van het internet welke meest worden gebruikt voor online piraterij. BitTorrent verkeer wordt ingeschat verantwoordelijk te zijn voor 17.9% van al het Internet verkeer. Envisional schat in dat ongeveer 67.7% van dit BitTorrent verkeer niet-pornografisch content is waarop copyright berust (bijv. films, televisie-afleveringen, muziek, computerspellen en software).

Wat betreft illegale content in Nederland meldt Ernst & Young in haar ICT Barometer over Cybercrime (2011:11) dat 6% van de ondervraagde professionals aangeeft dat hun

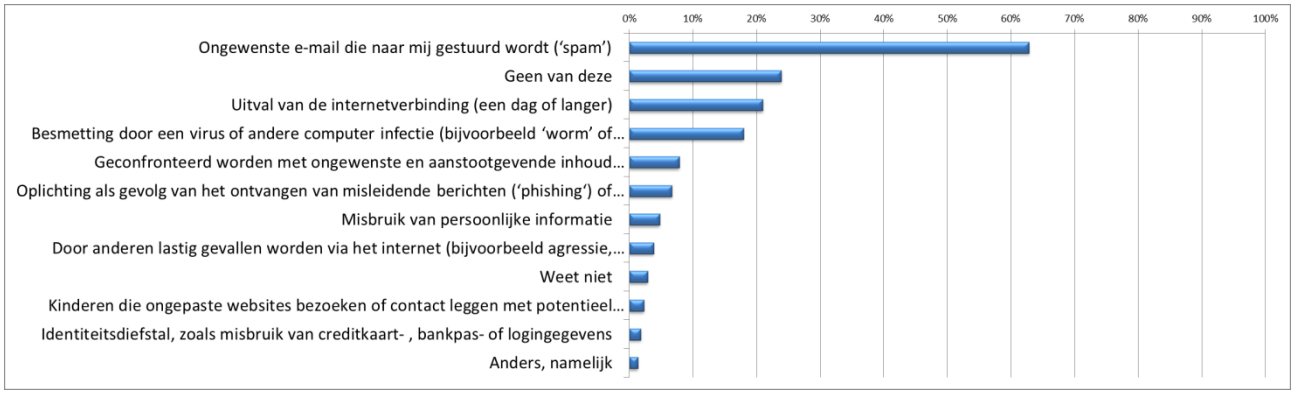
[22] Envisional is een bedrijf dat in opdracht van organisaties (bedreigingen) van piraterij, fraude en 'online brand abuse' opspoort en tegengaat.

organisatie te maken heeft gehad met het via hun computerstysteem verspreiden van illegaal materiaal (zie Figuur 57).



Figuur 57, Percentage respondenten dat meldt last te hebben gehad van o.a. verspreiden van illegaal materiaal via computersystemen van organisatie in 2011, Bron: Ernst & Young

In de TNO enquête uitgevoerd voor dit onderzoek is gevraagd naar de mate waarin de respondenten te maken hebben gehad met 'ongewenste content' (e.g. aanstootgevende content). Deze ongewenste content kan illegaal zijn (e.g. kinderporno), maar is niet per definitie illegaal. Het kan legale content betreffen die door de gebruiker als ongewenst wordt ervaren (e.g. geweldsbeelden). De onderstaande grafiek laat zien dat 8% van de respondenten in de eerste helft van 2012 te maken heeft gehad met ongewenste content, en 2% geeft aan dat ze meemaakten dat kinderen ongepaste websites bezochten of contact maakten met potentieel gevaarlijke personen.



Figuur 58, "Heeft u de afgelopen 6 maanden een of meer van de volgende problemen met privé-internetgebruik ervaren?"

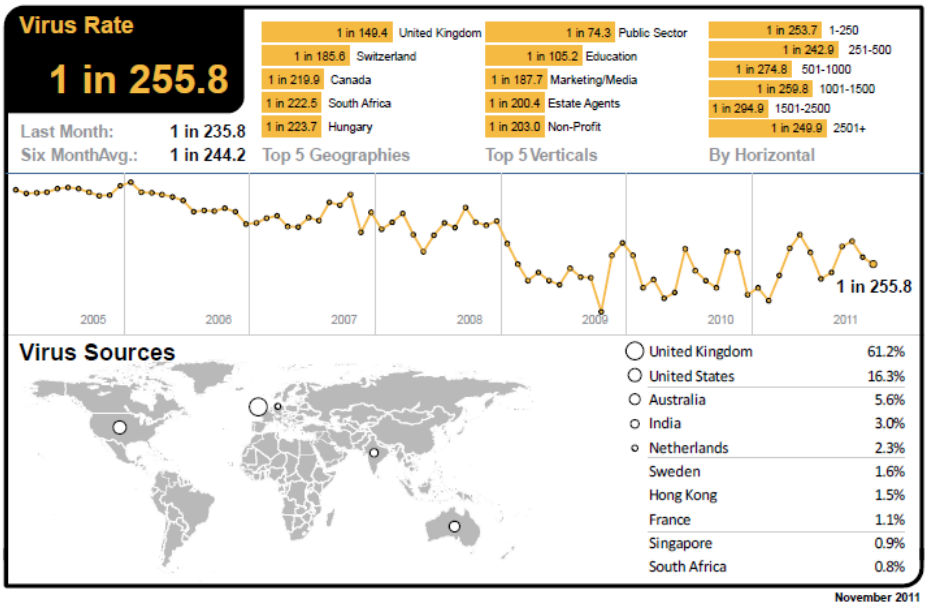
Bron: TNO enquete Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

5.2.4 *Malware*

Malware – malicious software, script of code – wordt ontwikkeld of gebruikt met als doel om informatie te vergaren (bijv. spyware, keylogger), specifieke berichten te verzenden (adware), toegang te krijgen tot een systeem (bijv. backdoor, rootkit), een systeem te besmetten met een virus (bijvoorbeeld bootsectorvirus), bepaalde verbindingen te leggen (bijv. dialer) of om op andere wijze schade aan te richten voor de gebruiker.

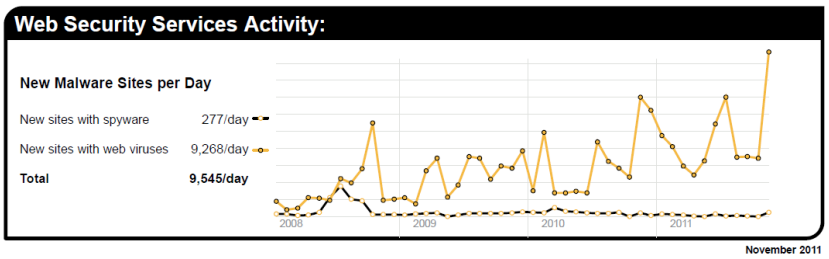
Zoals eerder gesteld, geldt ook voor malware dat het moeilijk is om betrouwbare cijfers over het volume in 2011 te genereren. Symantec geeft in haar malware analyse (2011:18) een overzicht van door hen gemeten virussen (via door hen geleverde beveiligingssoftware – zie paragraaf 3.2.5 voor beschreven methodiek) in 2011. In 2011 was 1 op de 255.8 emails gemeten door Symantec besmet met een virus (zie Figuur 59). In Nederland was dat

1 op de 238.2, waarmee Nederland iets boven het gemiddelde ligt. Over de algehele lijn lijkt het absolute aantal virussen over de jaren af te nemen, maar de fluctuatie toe te nemen. Dit zou mogelijk te maken kunnen hebben met het tegenwoordig sneller verspreiden van enkele invloedrijke virussen.



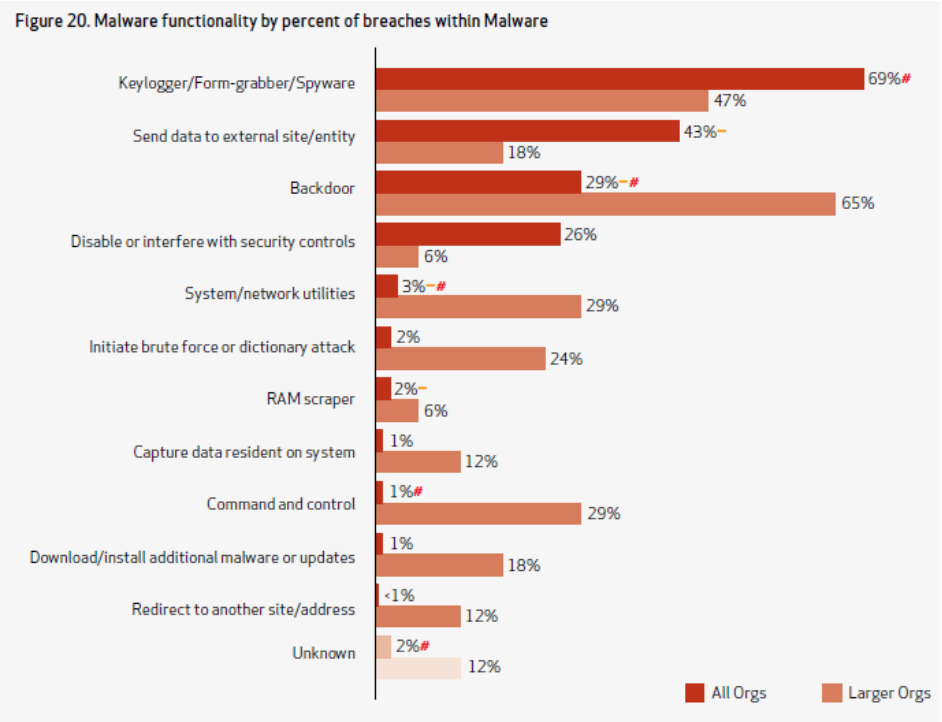
Figuur 59, Virus rate gemeten in verschillende landen in jaren 2005 tot en met 2011, Bron: Symantec

De volgende Figuur 60 laat de nieuwe malware websites per dag zien over de jaren 2008 tot en met 2011. Het lijkt dat hoewel het aantal sites met spyware redelijk stabiel is, de sites met web virussen een groei vertonen.



Figuur 60, Nieuwe malware sites per dag over de jaren 2001 tot en met 2011, Bron: Symantec

Verizon geeft in haar 'Data Breach Report' een overzicht van het type malware gevonden in 2011 dat werd gebruikt voor het lekken van data. Verizon vond in 2011 855 voorvallen van datalekken en de volgende Figuur 61 geeft aan welk percentage van de datalekken werd veroorzaakt door een specifiek type malware. De figuur laat zien dat de meeste breaches worden veroorzaakt door malware ontwikkeld om informatie te vergaren (keylogger, form-grabber, spyware) en door malware ontwikkeld om toegang te krijgen tot een systeem (backdoor).

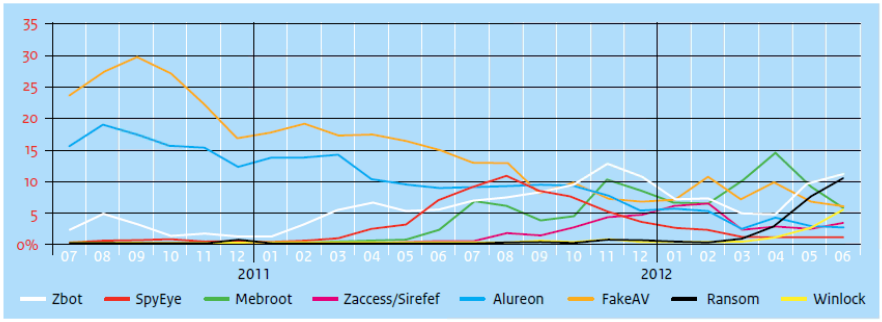


Figuur 61, Malware functionaliteit per percentage datalek door malware, Bron: Symantec

Wat betreft malware in Nederland, monitort het NCSC mogelijke malwarebesmettingen (2012:30). In 2011 en het eerste kwartaal van 2012 ontving het NCSC 2.400 meldingen over malware. Deze 2.400 meldingen hebben geresulteerd in 47 incidenten waarbij het NCSC bijstand heeft geleverd. De meeste van deze 47 incidenten betroffen malwareinfecties gerelateerd aan de Conficker en de Zeus-trojan.

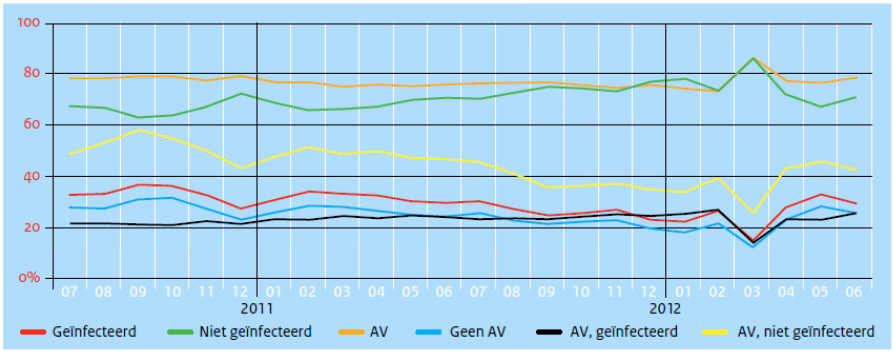
De organisatie Surfright, een Nederlandse leverancier van begeiligingsproducten, kwam met een overzicht van percentages per type malware in de jaren 2010 tot en met medio 2012 (gedetecteerd via het product HitmanPro – zie Figuur 62)[23]. In de metingen van Surfright nemen het aantal malware incidenten af, maar neemt één specifieke vorm van malware toe, namelijk ransomware. Ransomware heeft tot doel om de toegang tot een computersysteem te blokkeren en vraagt vervolgens een betaling om de blokkade op te heffen. In de registratie van Surfright was in het eerste half jaar van 2012 een toename te zien van het aantal incidenten waarbij ransomware betrokken was.

[23] Het is niet duidelijk wat het absolute aantal malware incidenten was en wat het totaal aantal onderzochte computers (met HitmanPro geinstalleerde software) was.



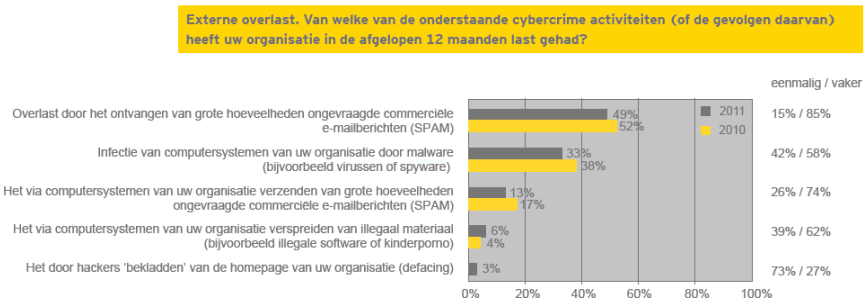
Figuur 62, Percentage malware per type over periode juli 2010 tot en met juni 2012, Bron: Surfright/NCSC

Wat betreft het aantal besmette PC's schatte SurfRight op basis van metingen via haar producten in dat het percentage schommelt rond de 30% over een periode van twee jaar (zie Figuur 63 hieronder).



Figuur 63, Infectiegraad Nederlandse PC's over periode juli 2010 tot en met juni 2012, Bron: Surfright/NCSC

De ICT Barometer over Cybercrime van Ernst & Young (2011) zien dat malware (naast Spam) nog steeds de grootste last veroorzaakt bij respondenten van de Barometer.
In 2011, antwoordde 33% van de respondenten in 2011 last te hebben gehad van malware (bijvoorbeeld virussen of spyware). Dit is 5% lager dan in 2010.



Figuur 64, Percentage respondenten dat in 2011 last had van o.a. malware, Bron: Ernst & Young

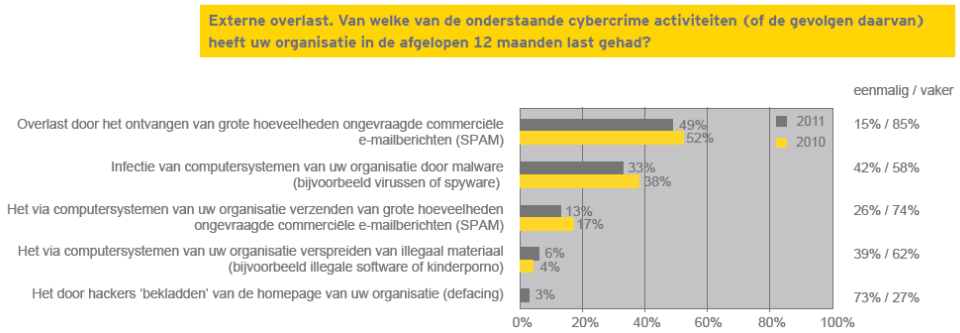
De TNO enquête uitgevoerd voor dit onderzoek laat zien dat ook gewone gebruikers relatief veel last hebben van virussen, namelijk 18% van de respondenten geeft dit aan voor de eerste helft van 2012, zoals in Figuur 33 weergegeven.

5.2.5 *Website defacement*

Website defacement kan worden begrepen als cybercriminaliteit waarbij de grafische vormgeving en/of tekst van de website wordt aangetast (veranderd). Hierbij wordt veelal

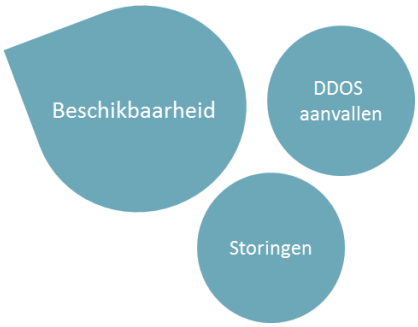
ingebroken op de webserver van de organisatie die doelwit is van de actie waarbij de website wordt vervangen door andere website.

Er zijn weinig betrouwbare statistieken te vinden over aantallen voorvallen van website defacement in 2011 in Nederland. Website defacement in de zin van het 'door hackers bekladden van een homepage' is wel door Ernst & Young meegenomen in hun ICT Barometer over Cybercrime (2011:11). Van de respondenten antwoordde 3% dat zij in 2011 last hadden gehad van deze vorm van defacement (zie Figuur 65).



Figuur 65, Percentage respondenten dat in 2011 last heeft gehad van o.a. het door hackers bekladden van de homepage van hun organisatie, Bron: Ernt & Young

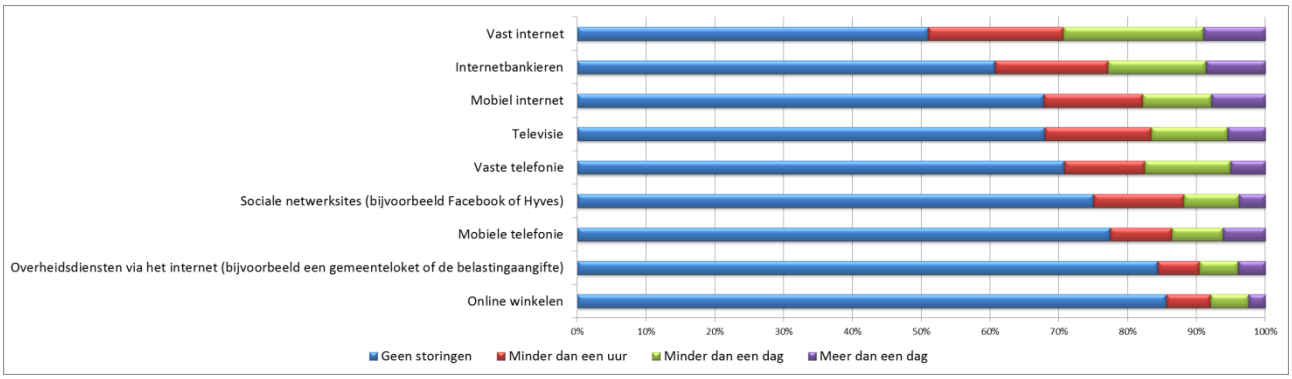
5.3 Beschikbaarheid



In deze paragraaf worden bestaande cijfers ten aanzien van 'beschikbaarheid' (van applicaties, informatie en diensten voor gebruikers) gepresenteerd.

5.3.1 Storingen

De TNO enquête uitgevoerd voor dit onderzoek geeft inizcht in de mate Nederlanders in de eerste helft van 2012 te maken hebben gehad met storingen. De volgende grafiek geeft een overzicht per type dienst.



Figuur 66, "Hoe lang heeft u van de onderstaande diensten geen gebruik kunnen maken door een technische storing in de afgelopen 6 maanden?"

Bron: TNO enquete Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

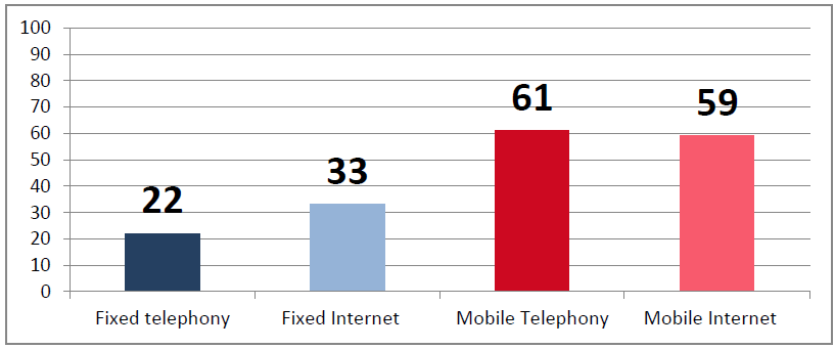
Storingen bij gebruik van vast internet en internetbankieren kwamen het meest voor. Een verklaring hiervoor kan zijn dat dit diensten zijn waarbij beschikbaarheid van groter belang is voor burgers dan bij bijvoorbeeld online winkelen of een overheidsloket. Een storing hierbij zal dan ook sneller opgemerkt en onthouden worden. Over het algemeen lijkt de onderbreking van beschikbaarheid van de meeste ICT diensten waar hier naar gevraagd is niet heel groot: minder dan 10% geeft aan meer dan een dag in de afgelopen 6 maanden een storing gehad te hebben.

Sinds 2012 is het middels de Telecomwet voor aanbieders van openbare netwerken en diensten verplicht om storingen te melden bij het Agentschap Telecom, wat hiervoor een speciale website heeft ingericht.[24] Voor 2012 heeft dit nog geen data over storingen opgeleverd, maar mogelijk dat dit voor de monitor 2013 waardevolle inzichten kan opleveren. Deze gegevens worden jaarlijks aan de Europese Commissie en ENISA doorgegeven.

Voor 2011 heeft ENISA al wel data informatie beschikbaar in haar jaarraport, die betrekking hebben op Europa. Een aantal belangrijke conclusies die ENISA met betrekking

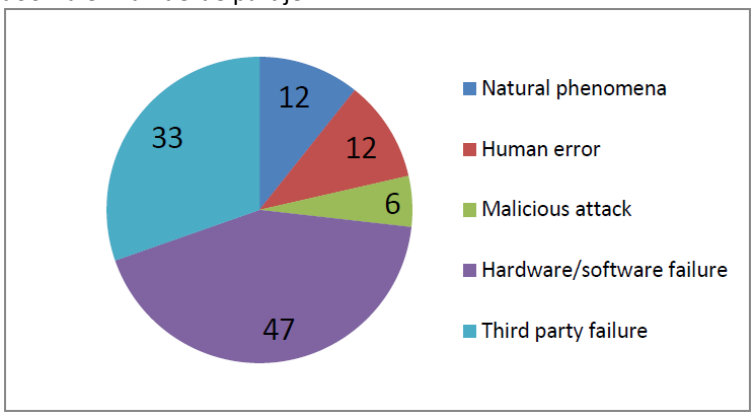
[24] Zie http://www.meldplichttelecomwet.nl/

tot de meldingen over storingen in de ICT infrastrutuur zijn dat de meeste meldingen mobiele telefonie of mobiel internet betroffen (60% van de incidenten):



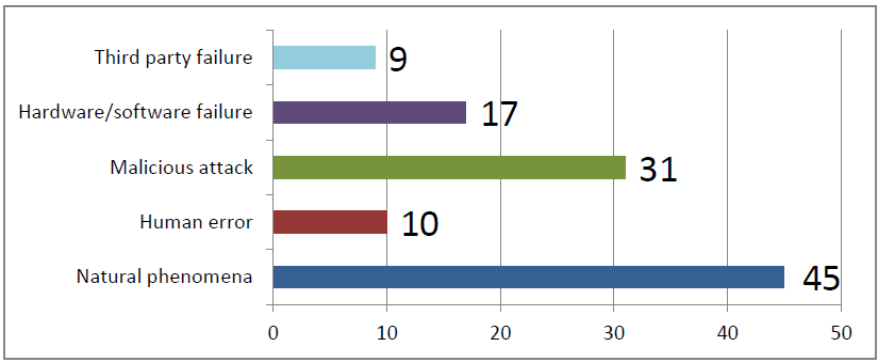
Figuur 67, Percentage incidenten per dienst. Bron: ENISA, 2012

Van deze storingen ondervonden ook de grootste aantallen gebruikers overlast (rond de 300.000). De meeste incidenten werden veroorzaakt door hardware of software falen, of door falen van derde partijen:



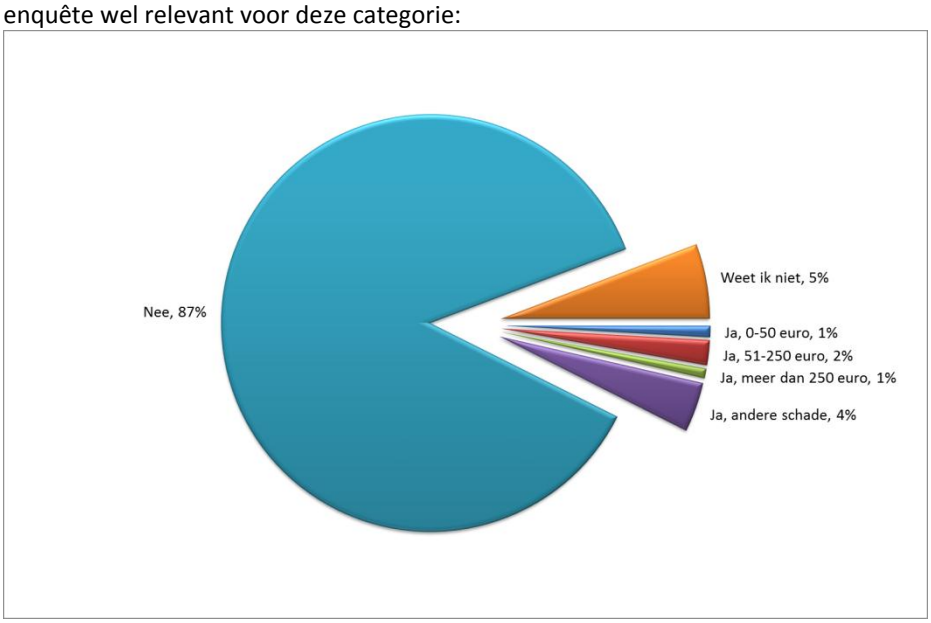
Figuur 68, Percentage incidenten per oorzaak. Bron: ENISA, 2012

Een sterke afhankelijkheid van de energievoorziening bleek ook een belangrijke factor te zijn bij storingen, vooral bij storingen als gevolg van natuurlijke fenomenen zoals overstromingen of zware sneeuwval. Deze storingen bleken ook gemiddeld het langst te duren:



Figuur 69, Gemiddelde duur incident per oorzaak in uren. Bron: ENISA, 2012

Tot slot, hoewel niet exclusief gericht op beschikbaarheid is de volgende vraag uit de TNO enquête wel relevant voor deze categorie:



Figuur 70, "Heeft u de afgelopen 6 maanden schade opgelopen door problemen bij internet gebruik?"

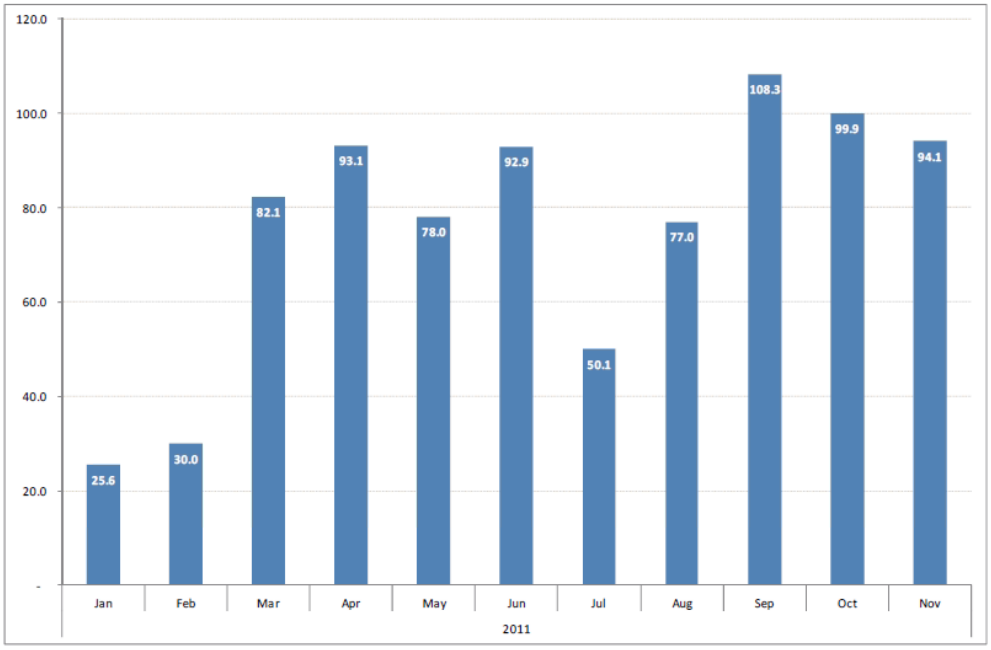
Bron: TNO enquete Veiligheid en Vertrouwen in ICT 2012 (N= 1042)

In de "Ja, andere schade" categorie hebben respondenten ook een reeks antwoorden gegeven, waarbij opvallend vaak ook zaken als "beschadiging harde schijf", "computer kapot", "crach van de disk" genoemd werden. Blijkbaar heeft men deze vraag ook geïnterpreteerd als algemene schade tijdens gebruik van ICT, zoals defecte computerhardware. Het deel van de respondenten die dus daadwerkelijk aangeeft schade te hebben geleden als gevolg van of bij het gebruik van ICT ligt onder de 8%, bij elkaar opgeteld.

5.3.2 DDOS Attacks

Een vorm van cybercrime welke tot doelwit de beschikbaarheid van diensten heeft, zijn Distributed Denial of Service Attacks (DDoS Attacks). Een DDoS attack is een aanval die door middel van een groot netwerk van (veelal gehackte) computers wordt uitgevoerd. Bij deze aanval wordt een internetdienst (bijv. een specifieke website) overspoeld met grote hoeveelheden netwerkverkeer zodat deze niet meer bereikbaar is voor normaal gebruik (Sommer and Brown, 2011).

Symantec bracht de via hun beveiligingsproduct Symantec.cloud gedetecteerde aanvallen voor 2011 in kaart (voor een beschrijving van de werkwijze van Symantec zie paragraaf 3.2.5). De volgende figuur laat voor 2011 het gemiddeld aantal tegengehouden aanvallen door Symantec.cloud per dag zien.

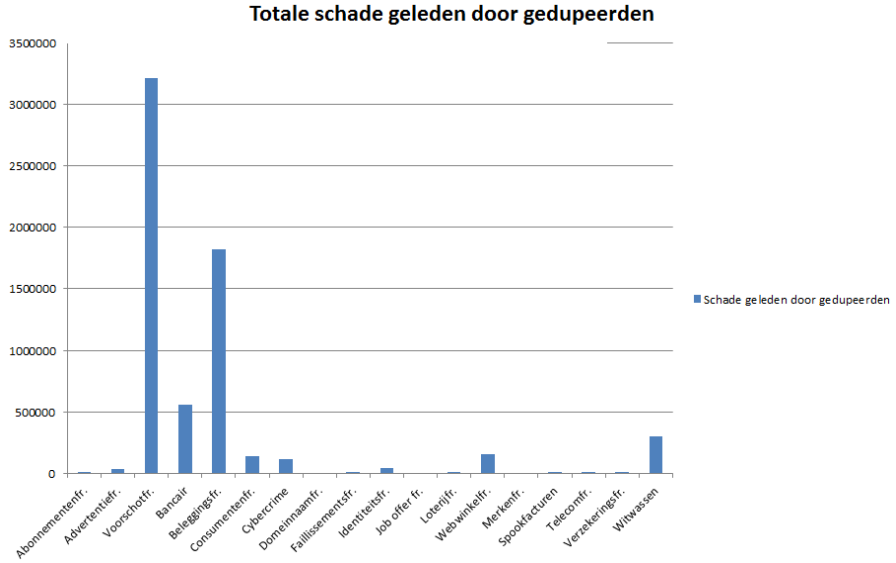


Figuur 71, Gemiddeld aantal trageted attacks tegengehouden door Symantec.cloud per dag wereldwijd in 2011, Bron: Symantec

5.4 Algemene cijfers cybercrime

De veiligheid van ICT wordt veelal in kaart gebracht door het verzamelen van gegevens over voorvallen van onveilige ICT. Situaties van onveilige ICT vallen in veel studies onder de noemer *cybercrime*. Cybercrime is een term die wordt gebruikt om een breed scala aan verschillende criminele activiteiten te beschrijven die gerelateerd zijn aan digitale data, computers en/of informatiesystemen (Shinder et al., 2008). Het is belangrijk om voorafgaand aan het presenteren van cijfers te vermelden dat onderzoekers wereldwijd aangeven dat het moeilijk is om betrouwbare statistieken te genereren (zie bijv. Florencio and Herly, 2011). Het probleem van gebrek aan betrouwbare data kent verschillende oorzaken. In de eerste plaats blijkt cybercrime vaak *under-reported* te zijn. Ferwerda et al. (2010) stellen bijvoorbeeld dat individuen niet gewend zijn om voorvallen van cybercrime te melden. Daarbij komt dat het per individu vaak gaat om kleine bedragen (denk aan fraude via Marktplaats) waarbij betrokkenen het niet de moeite vinden om het te melden[25]. Als het gaat om de private sector, worden cybercrime incidenten vaak niet gemeld omdat organisaties bang zijn voor reputatieschade en/of het wegblijven of weggaan van klanten (zie bijv. Jamieson et al., 2008).

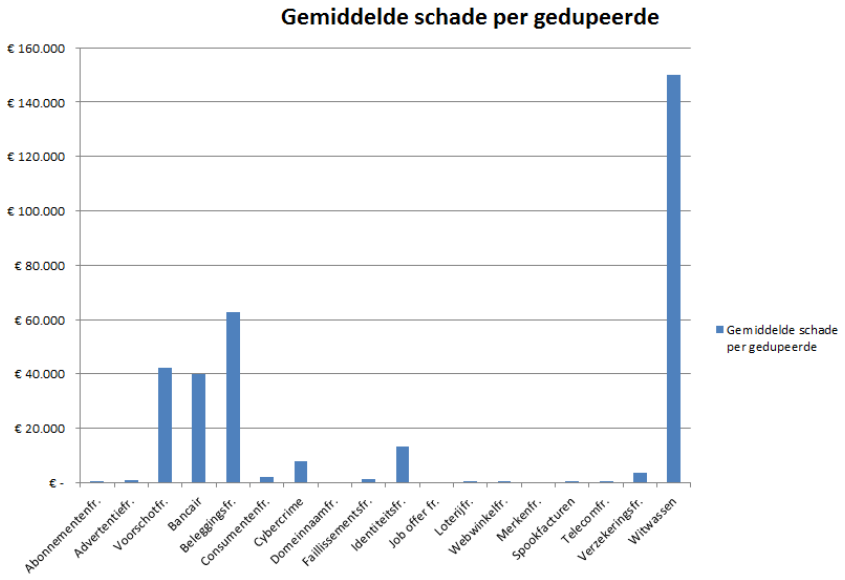
De schade die geleden wordt door cybercrime en webwinkelfraude lijkt relatief laag te zijn. Onderstaande figuur, gebaseerd op cijfers van de Fraudehelpdesk laat zien dat de fraudevormen 'voorschotfraude' en 'beleggingfraude' de hoogste schadeposten kennen. Beperkte schade voor eindgebruikers in het domein cybercrime kan mogelijk verklaard worden doordat klanten van banken veelal schadeloos gesteld worden (bijvoorbeeld bij pharming). De beperkte schade in het domein webwinkelfraude kan mogelijk verklaard worden doordat het om relatief kleinere bedragen gaat.



Figuur 72, Totale schade geleden door gedupeerden per fraudetype, Bron: Fraudehelpdesk

De onderstaande figuur laat de gemiddelde schade per gedupeerde zien. De Fraudehelpdesk kreeg in 2011 12 meldingen van witwassen waarbij 2 personen gedupeerd waren (voor gemiddeld bedrag van 150.000 euro per persoon).

[25] Het aantal gedupeerden is echter vaak groot.



Figuur 73, Gemiddelde schade per gedupeerde per fraudetype, Bron: Fraudehelpdesk

Cybercrime cijfers gebaseerd op een survey in 2011 worden daarnaast geleverd door het bedrijf Norton in hun rapportage 'Norton Cybercrime Report 2011'. Norton is een onderdeel van het bedrijf Symantec en levert beveiligingsproducten aan consumenten. Het onderzoek van Norton vond plaats in februari en maart 2011 waarbij 12.704 volwassenen in 24 landen, waaronder Nederland, werden ondervraagd. Norton geeft aan dat de gegevens zo gewogen zijn dat alle landen even sterk vertegenwoordigd worden. In Nederland zijn 512 volwassenen, 200 kinderen en 100 onderwijzers ondervraagd. Het is niet duidelijk hoe de precieze democrafische spreiding was[26]. Daarnaast is niet duidelijk hoe en welke vragen gesteld zijn. Onder cybercrime verstaat Norton alle mogelijke criminele activiteiten waarbij ICT wordt gebruikt ('computer viruses and malware, phishing, online harassment, social networking profile hacked, online sexual predators, online scams, credit card fraud, identity theft, smishing, other mobile phone cybercrime, other computer cybercrime').

Norton meldt in haar rapport dat:

- Norton inschat dat van april 2010 tot en met maart 2011 2,4 miljoen mensen in Nederland het slachtoffer waren van enige vorm van cybercriminaliteit.
- De kosten van april 2010 tot en met maart 2011 voor direct financieel verlies onder Nederlandse slachtoffers worden door Norton geschat op 249, 5 miljoen euro.
- Schade geleden doordat Nederlandse slachtoffers van april 2010 tot en met maart 2011 tijd verloren aan cybercriminaliteit schat Norton op 162,4 miljoen euro.
- Norton schat in dat 41% van de volwassenen die online actief zijn weleens slachtoffer geweest is van cybercrime (bijvoorbeeld virussen, malware, phishing, hacken en online scams).

Van de ondervraagde Nederlandse personen meldt 33% weleens te maken hebben gehad met virussen of malware, 5% met phishing, 5% met hacken van sociale netwerken en 1% met online scams. Daarnaast hebben de volgende percentages van de ondervraagde Nederlanders van april 2010 tot en met maart 2011 te maken gehad met de volgende typen cybercrime:

[26] Een sample van 512 bij een target populatie van 12 miljoen volwassenen in Nederland is bijvoorbeeld voldoende wanneer de demografische spreiding van de sample overeenkomt met de demografische spreiding van de target populatie.

	Nederland:	Wereldwijd:
Computervirussen en malware	18%	31%
Phishing	2,9%	5,3%
Hacken van sociale netwerken	2,1%	5%
Online scams	0,43%	5,7%

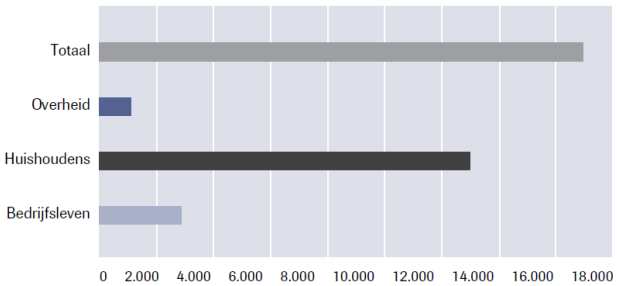
Tabel 7, percentage van ondervraagden dat in aanraking kwam met specifiek type cybercrime tussen april 2010 en maart 2011, Bron: Norton

Dat Nederlanders vooral last hebben gehad van virussen en Spam, blijkt ook uit de voor dit onderzoek uitgevoerde enquête. De eerder genoemde Figuur 25 geeft een overzicht van het percentage respondenten dat in de eerste helft van 2012 te maken had met specifieke vormen van cybercrime.

Norton geeft naast percentages van vormen van cybercrime ook een indicatie van de financiele kosten voor Nederlanders. Norton berekend dit door het aantal slachtoffers (inschatting op basis van survey) van de afgelopen jaren in een land te vermenigvuldigen met de gemiddelde financiele kosten van cybercrime. Hoe de gemiddelde financiele kosten van cybercrime zijn berekend is niet duidelijk. Dit is mogelijk gebeurd op basis van de survey (door aan respondenten te vragen wat de schade was, dit op te tellen en te delen door het aantal respondenten dat schade had).

De totale schade op jaarbasis voor huishoudens wordt geraamd op circa 13 miljard euro (WODC, 2010:244). Hiervan betreft ruim 2,4 miljard euro materiële schade, waarbij diefstal en vandalisme de grootste schadeposten zijn. De medische kosten als gevolg van slachtofferschap door criminaliteit worden geschat op 4,8 milard euro en de emotionele en fysieke schade op 5,7 miljard euro. De geraamde 411,9 miljoen euro schade voor Nederlandes burgers (bestaande uit 249,5 miljoen euro financieel verlies en 162,4 miljoen euro schade door tijdsverlies voor Nederanders) als gevolg van cybercrime, zoals berekend door Norton, lijkt hiermee relatief beperkt deel van de totale schade. Deze vergelijking lijkt erop te wijzen dat traditionele delicten (bijv. inbraak in woning, diefstal in publieke ruimten en vernieling) nog steeds veruit de meeste schade voor Nederlandse huishoudens veroorzaken en/of dat Nederlandse burgers niet direct de schade ondervinden aan vormen van cybercrime (bijvoorbeeld doordat ze schadeloos gesteld worden door banken).

Figuur 10.1 Maatschappelijke schade op jaarbasis, in mln euro, prijzen 2009



Voor de corresponderende cijfers zie tabel 10.1 in bijlage 4.
Bron: beheersverslag Belastingdienst/jaarverslag FIOD-ECD, jaarverslag AID, jaarverslag SIOD/SZW, jaarverslag SZW, jaarverslag VROM-IOD, diverse gemeenten, Meerding (2005), CBS, KLPD (2008), Monitor Criminaliteit Bedrijfsleven, Verbond van verzekeraars/centrum bestrijding verzekerings-fraude/Zorgverzekeraars Nederland, EnergieNEd., Nederlandse Vereniging van banken, Thuiswinkel Waarborg; bewerking WODC

Figuur 74, Maatschappelijke schade op jaarbasis, in mln euro, prijzen 2009, Bron: WODC

6 Conclusie

In dit onderzoek is getracht om zowel het vertrouwen van Nederlanders in ICT als de veiligheid van ICT in kaart te brengen. De onderzoeksresultaten laten zien dat het vertrouwen van Nederlanders in ICT over het algemeen hoog is. Hoewel 63% van de Nederlanders zich soms zorgen maakt over een mogelijk probleem of nadeel van Internet gebruik, weerhoudt dit Nederlanders er niet van om intensief gebruik te maken van het Internet o.a. voor sociale contacten, online winkelen en online bankieren. De meeste zorgen maken Nederlanders zich over besmetting van hun PC, Spam en misbruik van hun persoonlijke informatie (bij alle drie geeft 76% aan zich hier soms tot vaak zorgen om te maken). Ook is het percentage Nederlanders dat zich zorgen maken over uitval van de Internetverbinding, identiteitsdiefstal of phishing relatief hoog (respectievelijk 73%, 65% en 64%).

Het percentage Nederlanders dat diensten niet gebruikt vanwege beperkt vertrouwen ligt bij alle in de enquête opgenomen diensten (online winkelen, online advertenties, overheidsdiensten, sociale netwerksites, internetbankieren) onder de 8%, waarbij online advertenties het meest gemeden werden vanwege gebrek aan vertrouwen (8%) en (vaste) infrastructurele diensten en overheidsdiensten het minst gemeden werden (minder dan 3%). Daarnaast leiden eventuele zorgen van Nederlanders rond Internet gebruik slechts in beperkte zin tot het afzien van bepaalde activiteiten op het het Internet. Uit een andere vraag blijkt dat het percentage Nederlanders dat bepaalde activiteiten niet ondernam vanwege beperkt vertrouwen bij alle activiteiten onder de 14% ligt. Een activiteit die het meest gemeden werd was downloaden (14%.) en een activiteit die het minst gemeden werd was het communiceren met de overheid (5%).

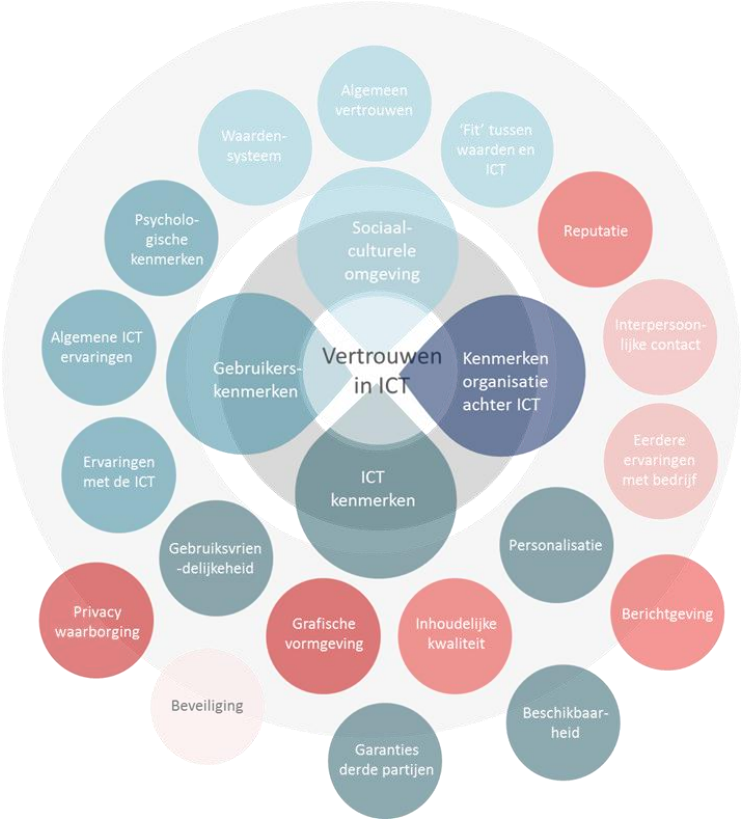
Van de personen die afzien van het gebruik van een dienst wegens onvoldoende vertrouwen in de veiligheid geeft de grootste groep (35%) als reden ‘zorgen om privacy’. Daarnaast worden een ‘onbetrouwbaar uiterlijk’ van een website (23%) en ‘slecht in het nieuws geweest zijn’ (19%) als redenen genoemd. Interessant is dat terwijl een meerderheid van de Nederlanders zich soms zorgen maakt over ernstigere problemen bij Internet gebruik – denk aan phishing, misbruik van gegevens, deze ernstigere problemen vrij weinig voorkomen. Het percentage Nederlanders dat daadwerkelijk ernstigere problemen ervaart met Internet gebruik (e.g. phishing, misbruik gegevens, online bedreiging) ligt bij al deze vormen onder de 10%. Nederlanders komen daarentegen wel regelmatig in aanraking met lichtere problemen of nadelen van Internet gebruik in aanraking, namelijk besmetting (of poging tot besmetting) van PCs (18%), het ontvangen van ongewenste email (63%) en de uitval van de Internetverbinding (21%).

De voorgaande resulaten uit the TNO enquête zijn in lijn met de cijfers voortvloeiend uit het dataonderzoek naar feitelijke (on)veiligheid en cybercrime. Deze laatste cijfers laten ook zien dat het aantal Nederlandse burgers dat te maken krijgt met lichtere vormen van cybercrime (bijv. Spam) relatief hoog is, maar dat het aantal dat te maken krijgt met ernstigere vormen (bijv. phishing) vergelijkbaar is met het percentage Nederlanders dat slachtoffer is van ‘off-line’ criminaliteit. Ook lijken de cijfers erop te wijzen dat de schade die burgers hebben naar aanleiding van ‘off line’ criminaliteit (bijv. diefstal zonder gebruikmaking van ICT, inbraak, misleiding, zakkenrollen) groter is dan de schade die zij lijden aan vormen van cybercrime. Hierbij is het belangrijk om te blijven vermelden dat dit een vertekend beeld kan zijn, omdat niet alle computercriminaliteiten door burgers gemeld worden. Daarnaast worden slachtoffers (bijv. van phishing) veelal schadeloos gesteld, waardoor zij minder schade lijden aan vormen van cybercrime.

In het bedrijfsleven lijken vooralsnog de grotere bedrijven werkzaam in de financiële sector substantiële schade aan vormen van cybercrime (bijv. phishing, skimming en hacken) te ondervinden. Ook de film- en muziekindustrie lijken proportioneel meer getroffen te worden dan andere industrieën (door illegaal downloaden). Hoewel grotere bedrijven over het algemeen beter beveiligde systemen hebben, zit hier meer vermogen en (waardevolle) gegevens en zijn zij daarmee een aantrekkelijk doelwit. De ICT Barometer over Cybercrime van Ernst & Young laat eenzelfde beeld zien. Terwijl van de grote ondernemingen (500+ werknemers) 49% in 2011 schade ondervond door vormen van cybercrime (door Ernst & Young breed geïnterpreteerd, hieronder valt ook Spam) was dat bij kleinere bedrijven (1-19 werknemers) 24%. MKB lijkt vooralsnog vooral last te hebben van traditionele vormen van criminaliteit (diefstal zonder gebruik ICT, inbraak en vernieling). Ook hier geldt weer dat het beeld vertekend kan zijn door beperkte (kwaliteit van de) data.

Vrijwel alle voor dit onderzoek geraadpleegde registraties laten eenzelfde trend over de afgelopen jaren zien; namelijk een toename van cybercrime incidenten. Omdat ICT steeds meer vervlochten is in het dagelijks leven, is het waarschijnlijk dat cybercrime een steeds grotere deel gaat uitmaken van de totale criminaliteit. Met name nieuwe technologieën kunnen hierbij kwetsbaar zijn, omdat deze in het beginstadium vaak nog niet optimaal beveiligd zijn en/of tactieken van criminelen bij gebruikers nog niet bekend zijn.

Tot slot is opvallend dat wanneer we de onderzoeksresultaten ten aanzien van vertrouwen confronteren met de onderzoeksbevindingen van veiligheid, het vertrouwen van Nederlanders in ICT slechts in zeer beperkte mate afhangt van de feitelijke veiligheid van de ICT. De onderstaande figuur geeft een overzicht van factoren die het vertrouwen van gebruikers in ICT het meest beïnvloeden (hoe donkerder rood, hoe dominanter; blauwe factoren zijn in deze monitor niet gemeten).



7 Literatuur, documenten en websites

Literatuur

- Aiken, K.D. and D.M. Bousch, (2006), Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context specific nature of internet signals, in: Journal of the Academy of Marketing Science, Volume 34, pages 308-323
- Arcand, M., Nantel, J., Arles-Dufour, M. and A. Vincent, (2007), The impact of reading a Web site's privacy statement on perceived control over privacy and perceived trust, in: Online Information Review, Volume 31, Issue 3, pages 661-681
- Ark, B. van, O'Mahony, M. and M.P. Timmer, (2009), The Productivity Gap between Europe and the United States: Trends and Causes, in: Journal of Economic Perspectives, Vol. 22, Nr. 1, pp. 25-44
- Bart, Y., Shankar, V., Sultan, F. and G.L. Urban, (2005), Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study, in: Journal of Marketing, Volume 69, pages 133-152
- Beldad, A., (2011), Trust and information privacy concerns in electronic government, PhD Dissertation, University of Twente
- Bente, G., Baptist, O. and H. Leuschner, (2012), To buy or not to buy: influence of seller photos and reputation on buyer trust and purchase behavior, in: International Journal of Human-Computer Studies, Volume 70, Issue 1, pages 1-13
- Bus, J., (2005), Building trust and security in information society: a strategic challenge for European RandD, ERCIM News Online Edition, ERCIM News 63
- Briggs, P., Simpson, B. and A. de Angeli, (2004), Personalisation and trust: A reciprocital relationship? In: Karat, C.M., Blom, J.O. and J. Karat (eds), Designing personalized user experiences in e-commerce, Kluwer, pages 39-55
- Corritore, C.L., Kracher, B. and S. Wiedenbeck, (2003), On-line trust: concepts, evolving themes, a model, in: International Journal of Human-Computer Studies, Volume 58, Issue 6, pages 737-758
- Doney, P.M., Cannon, J.P. and M.R. Mullen, (1998), Understanding the influence of national culture on the development of trust, In: Academy of Management Review, Volume 23, Issue 3, page 601-620
- Ferwerda, J., Choucri, N. and S Madnick, (2010), Institutional foundations for cyber security: current responses and new challenges, Working Paper, Cambridge MA
- Florencio, D. and C. Herley, (2011), Sex, Lies and Cybercrime Surveys, Microsoft Research
- Gefen, D., (2000), E-commerce: The roles of familiarity and trust, in: Omega, Volume 28, pages 725-737
- Gefen, D. and D.W. Straub, (2004), Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services, in: Omega, Volume 32, Issue 5, pages 407-424
- Hoffman, D.L., Novak, T.P. and M.A. Peralta, (1999), Information privacy in the marketplace: Implications for the commercial uses of anonymity on the Web, in: The Information Society, Volume 15, pages 129-139
- Jamieson, R., Land, L., Stephens, G. and D. Winchester, (2008), Identity crime: the need for an appropriate government strategy, Forum on Public Policy/A Journal of the Oxford Round Table
- Jøsang, A., Ismail, R. and C. Boyd, (2007) A survey of trust and reputation systems for online service provision, in: Decision Support Systems, Volume 43, Issue 2, pages 618-644

- Kim, J. and J.Y. Moon, (1998), Designing towards emotional usability in customer interfaces: Trustworthiness of cyber-banking system interfaces, in: Interacting with Computers, Volume 10, pages 1-29
- Kirs, P. and K. Bagchi, (2012), The impact of trust and changes in trust: A national comparison of individual adoptions of information and communication technologies and related phenomenon, in: International Journal of Information Management, in press corrected proof
- Koehn, D., (2003), The nature of and conditions for online trust, in: Journal of Business Ethics, Volume 43, pages 3-19
- Lai, I.K.W., Tong, W.L.V and D.C.F. Lai, (2011), Trust factors influencing the adoption of internet-based interorganizational systems, in: Electronic Commerce Research and Applications, Volume 10, Issue 1, pages 85-93
- Lauer, T.W. and X. Deng, (2007), Building online trust through privacy practices, in: International Journal of Information Security, Volume 6, pages 323-331
- Lee, Ch. S. and L. Ma, (2012), News sharing in social media: The effect of gratifications and prior experience, in: Computers in Human Bevior, Volume 28, Issue 2, pages 331-339
- Liao, C., Palvia, P. and H.N. Lin, (2006), The roles of habit and website quality in ecommerce, in: International Journal of Information Management, Volume 26, pages 469-483
- Mayer, R.C., Davis, J.H. and F.D. Schoorman, (1995), An integrated model of organization trust, in: Academy of Management Review, Volume 20, Issue 3, pages 709-734
- O'Reilly, P. and P. Finnegan, (2005), Performance in electronic marketplace: theory in practice, in: Electronic Markets, Volume 15, Issue 1, pages 23-37
- PWC, (2011), Omvang van identiteitsfraude & maatschappelijke schade in Nederland, Amsterdam
- Saila, H., O'Keefe, R.M. and K.S. Hone, (2004), The impact of religious affiliation on trust in the context of electronic commerce, in: Interacting with Computers, Volume 16, Issue 1, pages 7-27
- Shankar, V., Urban, G.L. and F. Sultan, (2002), Online trust: A stakeholder perspective, concepts, implications, and future directions, in: Journal of Strategic Information Systems, Volume 11, pages 325-344
- Shinder, L. and M. Cross, (2008), Facing the Cybercrime Problem Head-On, Scene of the Cybercrime (second edition), pp. 1-39
- Sommer, P. and I. Brown, (2011), Reducing systemic cybersecurity risk, As of 19 February
- Sparks, B.A. and V. Browning, (2011), The impact of online reviews on hotel booking intentions and perception of trust, in: Tourism Management, Volume 32, pages 1310-1323
- Toutenhoofd-Visser, M.H., Veenstra, S., Domenie, M.M.L., Leukfeldt, E.R. en W. Ph. Stol, (2009), Politie en Cybercrime, Intake en Eerste Opvolging, Een onderzoek naar de intake van het werkaanbod cybercrime door politie, Lectoraat Cybersafety, Noordelijke Hogeschool Leeuwarden
- Yoon, Ch. (2009), The effects of national culture values on consumer acceptance of e-commerce: Online shoppers in China, in: Information & Management, Volume 46, Issue 5, pages 294-301

Rapporten

- AIVD, (2011), Jaarverslag 2011, Zoetermeer
- APWG, (2011), Phishing Activity Trends Report, 1st Half 2011, USA
- APWG, (2011), Phishing Activity Trends Report, 2nd Half 2011, USA
- Cabinet Office, (2009), Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space, London

- Cap Gemini (2011), Trends in Veiligheid 2011-2012, Veranderende rollen voor overhead, bedrijfsleven én burger, Utrecht
- CBP, (2011), Jaarverslag 2011, Den Haag
- CPNI, Platform voor Cybersecurity, Jaarbericht 2011, Den Haag
- Considerati, (2011), Feiten om te delen, Digitale contentdistributie in Nederland, Amsterdam
- CVV, Trend-Signalement 2012, 20 ontwikkelingen in maatschappelijke veiligheid, Utrecht
- DNB, (2011), Rapportage Maatschappelijk Overleg Betalingsverkeer 2011, Amsterdam
- Enisa, (2011), Survey of accountability, trust, consent, tracking, security and privacy mechanisms in online environments, Brussels
- Enisa, (2012), Annual Incident Reports 2011, Brussels
- Envisional, (2011), Technical Report: An Estimate of Infringing Use of the Internet, Cambridge
- Ernst & Young, ICT Barometer over Cybercrime, Ernst & Young Nederland LLP, Amsterdam
- Garlik, (2009), UK Cybercrime Report, September 2009, Richmond, United Kingdom
- Govercert, (2010), Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010, Den Haag
- Govercert, (2011), Cybersecuritybeeld Nederland, December 2011, Den Haag
- ITRC, (2011), Identity Theft Resource Center, 2011 Data Breach Stats, USA
- ITU, (2008), Study on the Financial Aspects of Network Security: Malware and Spam, Geneva
- Ministerie Economische Zaken, Landbouw en Innovatie, (2011), Digitale agenda.nl, ICT voor innovatie en economische groei, Den Haag
- Ministerie van Veiligheid en Justitie (2010), De Nationale Cyber Security Strategie (NCSS), Slagkracht door samenwerking, Den Haag
- Ministerie van Economische Zaken, Landbouw en Innovatie, (2011), Digitale Implementatie Agenda, Den Haag
- NCSC, (2012), Cybersecuritybeeld Nederland, CSBN-2, Den Haag
- Norton, (2011), Norton Cybercrime Report, Mountain View, USA
- OECD, (2011), Society at a Glance 2011, OECD Social Indicators, OECD Publishing, Paris
- OPTA, (2012), Marktmonitor 2008 tot en met 2011, Den Haag
- Pew Internet & American Life Project, (2011), Teens, Kindness and Cruelty on Social Network Sites, Washington D.C.
- Pew Internet & American Life Project, (2012), The Tone of Life on Social Networking Sites, Washington D.C.
- PWC, (2011), Omvang van identiteitsfraude & maatschappelijke schade in Nederland, Amsterdam
- PWC, (2011), Cybercrime: protecting against the growing threat, Global Economic Crime Survey, London
- Robinson, N., Disley, E., Potoglou, D., Reding, A., Culley, D., Penny, M., Botterman, M., Carpenter, G., Blackman, C. and J. Millard, (2012), Feasibility study for a European Cybercrime Center, Final Report, TR-1218-EC, prepared for the European Commission, Brussels
- SEO, (2007), De kosten van criminaliteit, Een onderzoek naar de kosten van criminaliteit voor tien verschillende delicttypen, in opdracht van WODC, Den Haag
- Sociaal Cultureel Planbureau, (2012), Burgerperspectieven, 2012/1, COB, Den haag
- Symantec, (2011), Symantec Intelligence Report, November 2011, Mountain View, USA

- TNO, (2010), Het monitoren van vertrouwen in ICT op basis van cyber-indicators, Delft
- TNO, (2011), Monitor veiligheid en vertrouwen, Delft
- Verizon, (2011), Data Breach Investigations Report, New York City
- WODC, (2010), Criminaliteit en rechtshandhaving 2010, Ontwikkelingen en Samenhagen, Den Haag

Statistieken

- European Social Survey
- Eurostat
- Fraudehelpdesk
- CBS
- WODC
- World Values Survey

Websites:

- Anti-Phishing Working Group, http://www.antiphishing.org/
- BREIN, http://www.anti-piracy.nl/