Behavioural and Societal Sciences
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

R35601

Monitor veiligheid en vertrouwen

Datum	9 december 2011
Auteur(s)	Sander Degen Sanne Huveneers
Review	Robert Kooij
Aantal pagina's	44
	Deze rapportage maakt onderdeel uit van het monitorings-programma van TNO en is tot stand gekomen dankzij een bijdrage van het Ministerie van Economische Zaken, Landbouw en Innocatie
Projectnummer	055.01021/01.01.05

Inhoudsopgave

1 Inleiding

1.1 Achtergrond

Internet ontwikkelt zich in toenemende mate tot een vitale infrastructuur die de basis vormt voor economische en sociale processen binnen onze (informatie)maatschappij. In de vijftien jaar dat het World Wide Web bestaat, heeft het zich gemanifesteerd als een netwerk met diepgaande en transformatieve impact op bijna alle aspecten van onze samenleving. Belangrijke trends hierin zijn communicatie overal en altijd, sociale netwerken, brede en transparante informatievoorziening, en de ontwikkeling van talloze publieke en private digitale diensten.

De ontwikkeling van het internet is niet te stoppen en zal de komende jaren gaan zorgen voor veranderingen die verder reiken dan informatieverwerking en gegevensuitwisseling. Het “Internet of Things”, het semantische web en cloud computing zijn al in ontwikkeling waardoor de digitalisering van de maatschappij en ons leven nog meer een feit zal worden.[1] Het is van economisch en maatschappelijk belang de kansen die ICT ons biedt, optimaal te benutten.

Met deze toenemende impact van het internet op onze maatschappij en ons dagelijkse leven is onze afhankelijkheid van deze groeiende mogelijkheden steeds groter aan het worden, Maar hoewel deze nieuwe ontwikkelingen en deze nieuwe wereld ons soms verbazen, worden bedenkingen steeds vaker geuit jegens deze nieuwe wereld vol technologische mogelijkheden waarin ook de kansen voor criminelen om hier misbruik van te maken duidelijk aanwezig zijn.

Risico’s op en werkelijke incidenten met het misbruiken van gegevens zijn een feit: cybercriminelen die de zwakke plekken van netwerken opzoeken, terroristische organisaties die het internet gebruiken om informatie uit te wisselen en de inbreuk op data van organisaties en eindgebruikers. Persoonlijke en gevoelige gegevens, profielen en digitale identiteiten kunnen worden gestolen en worden doorverkocht.

De adoptie en het gebruik van digitale diensten en voorzieningen wordt beïnvloed door diverse factoren. Een van die factoren is het vertrouwen dat gebruikers hebben in de betreffende dienst. Wanneer het vertrouwen laag is, zal dit naar verwachting de adoptie negatief beïnvloeden. Andersom geldt dit ook; als het vertrouwen hoog is, zal dat geen reden zijn om de dienst niet te benutten. Uiteraard kunnen er andere redenen zijn om de dienst niet te gebruiken, bijvoorbeeld de beschikbaarheid van de dienst, de gebruiksvriendelijkheid en de kosten die met het gebruik gepaard gaan. Dat het belangrijk is om het vertrouwen in diensten te vergroten, blijkt onder andere uit onderzoek van Ernst &Young dat constateert dat een verbetering van het vertrouwen 1,2 miljard extra omzet kan opleveren voor internethandel in 2014[2]. Om dit te bewerkstelligen, is het nodig om te weten wat het vertrouwen in ICT bepaalt en welke factoren invloed hierop hebben. Ook is het noodzakelijk om de relatie tussen vertrouwen en de adoptie van digitale faciliteiten verder te onderzoeken.

Daarnaast is het interessant om het vertrouwen dat gebruikers stellen in digitale diensten en voorzieningen, te vergelijken met het daadwerkelijk risico dat gebruikers lopen bij het gebruik van ervan. De perceptie van het risico door gebruikers, kan afwijken van het feitelijke risico, waardoor twee problemen kunnen

[1] Trust in the Information Society, Riseptis, 2009
[2] Ernst & Young, Groeien door veiligheid, 2011

ontstaan: (1) Als er een lage risicoperceptie is en een hoog feitelijk risico, loopt de gebruiker door een onterecht vertrouwen een grote kans om schade op te lopen bij het gebruik van een dienst, (2) Bij een hoge risicoperceptie en een laag feitelijk risico, zal de gebruiker geneigd zijn de dienst niet te gebruiken waardoor de adoptie om ongegronde redenen achterblijft.

1.2 Doelstelling

Om meer inzicht te krijgen in de risico's bij het gebruik van ICT-diensten en de relatie met het vertrouwen van consumenten en bedrijven, is besloten te werken aan een monitor 'Vertrouwen in ICT'. Dit onderzoek heeft als doel de eerste noodzakelijke stap te zetten: het bouwen van een monitoringfundament om over langere periode het vertrouwen in ICT-diensten inzichtelijk te maken. Naast de ontwikkeling van een monitoring framework, heeft dit onderzoek ook als doel om inzicht te verkrijgen in het vertrouwen in e-Commerce.

Met deze resultaten wordt duidelijk welke informatie nog mist om de monitor verder uit te breiden naar andere cases. Ook kunnen de eerste resultaten leiden tot speerpunten waar extra aandacht van de overheid wenselijk is.

1.3 Onderzoeksvragen

De monitor die dit jaar wordt ontwikkeld zal de volgende onderzoeksvragen uitlichten:

- Welke veiligheidsrisico's spelen er bij het gebruik van ICT-diensten?
- Hoe groot is de risicoperceptie van deze veiligheid bij gebruikers van deze ICT-diensten?
- Welke invloed heeft deze risicoperceptie op het algehele vertrouwen?

Daarbij zal, dit jaar, met name worden ingezoomd op de case e-Commerce.

Daarnaast is het belangrijk om de ontwikkelingen in zowel de feitelijke risico's als de perceptie van gebruikers te monitoren, zodat gekeken kan worden of het vertrouwen in diensten verandert en welke maatregelen het risico of het vertrouwen zouden kunnen bijsturen.

1.4 Methode

Om bovenstaande doelstelling te behalen en een antwoord te kunnen geven op de onderzoeksvraag, worden diverse methodes ingezet.

Ontwikkeling monitoring framework
Het onderzoeksmodel dat wordt gehanteerd om de risico's en de perceptie van risico in kaart te brengen, moet geschikt zijn voor herhaling om te spreken van een monitor. Dit betekent dat er een set indicatoren moet worden benoemd om te meten welke risico's bij het gebruik van diensten gemeten worden, of worden gepercipieerd. Het monitoring framework zal inzicht geven in welke indicatoren het risico bepalen. Vervolgens kan per indicator een score worden benoemd, waardoor er een assessment plaats kan vinden. Het monitoring framework maakt daardoor inzichtelijk hoe groot de risico's zijn voor verschillende indicatoren en hoe dit zich verhoudt tot de perceptie.

Onderzoek naar feitelijke risico's
Er wordt literatuuronderzoek verricht om meer inzicht te krijgen in de feitelijke risico's bij het gebruik van ICT-diensten in het algemeen en e-Commerce in het bijzonder.

Onderzoek naar vertrouwen
In dit onderzoek zullen we via literatuuronderzoek informatie verzamelen over het vertrouwen van de gebruiker en meer specifiek naar hun perceptie van de gesignaleerde feitelijke risico's. We zullen kijken naar vertrouwen in het algemeen en naar e-Commerce in het bijzonder. Waar mogelijk zullen verbanden worden gelegd met de feitelijke situatie.

Om consumentenvertrouwen over langere periode te meten en te relateren aan specifieke gebeurtenissen, is het aan te raden om een eigen gebruikersonderzoek op te zetten. Door een survey kan ook beter bekeken worden door welke factoren het vertrouwen gestuurd wordt.

1.5 Leeswijzer

In het volgende hoofdstuk wordt de context van dit onderzoek nader toegelicht. We benoemen er kort welke definitie van 'vertrouwen' gehanteerd is en welke actoren en stakeholders een rol spelen. In hoofdstuk drie wordt de aanpak van het onderzoek gepresenteerd. Hoofdstuk vier en vijf bespreken respectievelijk de resultaten met betrekking tot de veiligheid van ICT diensten en het vertrouwen in deze diensten. Ten slotte worden in hoofdstuk zes de conclusies en aanbevelingen toegelicht.

2 Vertrouwen in ICT-diensten – Context

2.1 Definities van vertrouwen

Vertrouwen is een breed en lastig te vatten begrip. Waar vertrouwen precies door bepaald wordt, kan van persoon tot persoon verschillen en is vaak ook afhankelijk van het onderwerp of de situatie. Er zijn dan ook verschillende theorieën die verschillende niveaus van vertrouwen behandelen. In relatie tot dit onderzoek, onderscheiden we drie niveaus van vertrouwen:

2.1.1 Vertrouwen algemeen

Er zijn verschillende theorieën die beschrijven hoe vertrouwen tot stand komt, welke factoren op het vertrouwen van invloed zijn en wat het effect is van vertrouwen op het gedrag van een individu of groep. Huijboom (2010) beschrijft in haar proefschrift de drie eigenschappen van vertrouwen op basis van onderzoek van Edelenbos en Klijn (2007). Volgens deze definitie bestaat vertrouwen uit:

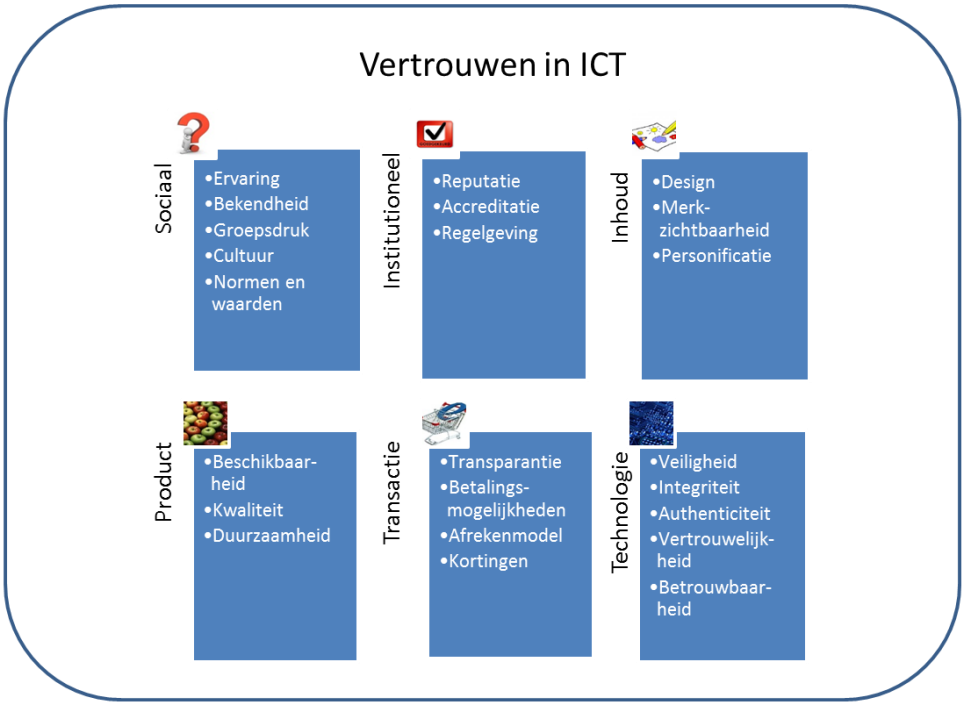
1. Kwetsbaarheid (*vulnerability*)
2. Risico (*risk*)
3. Verwachtingen (*expectations*)

De theorie gaat ervanuit dat om vertrouwen te hebben in een actor, men bereid is zich open en *kwetsbaar* op te stellen. Men durft er vanuit te gaan dat de andere partij geen opportunistisch gedrag laat zien dat ons kan schaden, ook al zou dat wel het geval kunnen zijn. In *risicovolle* situaties, is vertrouwen zelfs noodzakelijk. Ook vraagt vertrouwen een positieve *verwachting* ten aanzien van de motieven van de ander.

Deze driedeling laat zien dat de perceptie van risico en de perceptie van de motieven van andere actoren een belangrijke rol spelen bij het vertrouwen en de beslissing om met een partij in zee te gaan.

2.1.2 Vertrouwen in ICT-diensten

Wanneer we het vertrouwen onderzoeken in een specifieke context, blijven bovenstaande bouwstenen relevant, maar kunnen meer concrete factoren worden benoemd die het vertrouwen beïnvloeden. Kim e.a. (2005) en Corbitt e.a. (2003) onderscheidden verschillende vertrouwensdimensies. Hoewel het een uitwerking biedt van algemenere theorieën, zijn niet alle dimensies in elke onderzoek setting even relevant. Welke vertrouwensdimensies een rol spelen, is mede afhankelijk van het type **product of dienst** en de actoren die bij het gebruik van het product een rol spelen (zie ook 2.1.3).

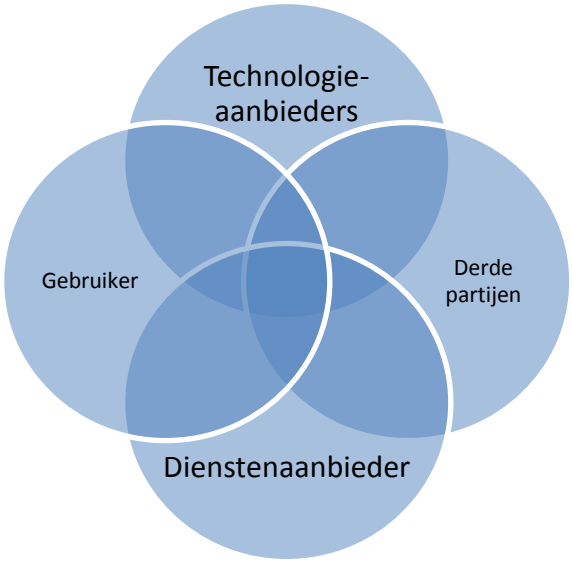


2.1.3 Invloed van feiten op het vertrouwen

In dit onderzoek kijken we nadrukkelijk naar de kloof tussen de veiligheid van ICT-diensten, de perceptie van deze veiligheid door gebruikers en de impact van deze perceptie op het algehele vertrouwen in de specifieke dienst. Als we het hebben over de feitelijke veiligheid van ICT-diensten, dan verwachten we vooral een relatie met de vertrouwensdimensies ‘technologie, transactie en product’.

2.2 Actoren en stakeholders

Er zijn diversen actoren die direct of indirect invloed hebben op het vertrouwen in een ICT dienst. Hoewel de actoren per dienst of product kunnen verschillen, kunnen de volgende algemene groepen worden onderscheiden:



Dienstenaanbieders
- De aanbieder van de gebruikte dienst.

Gebruikers:
- De afnemer van een dienst, dit kan zowel een consument zijn als een (ander) bedrijf.

Technologieaanbieders:
- Alle partijen die voor de technologie zorgen waarmee de dienstafname mogelijk is, bijvoorbeeld telecomoperators, computerfabrikanten, netwerkinfrastructuurleveranciers, telefoonproducenten, etc.

Derde partijen:
- Alle overige partijen die een faciliterende rol hebben bij het aanbod van een bepaalde dienst, bijv. een payment provider, pakketdienst, etc.

Afhankelijk van welke dienst gebruikt wordt, spelen verschillende actoren een rol. Voor veel spelers geldt dat zijn bij verschillende producten of diensten betrokken zijn en soms ook in verschillende rollen. Dit maakt de rol van de actor in de veiligheid van (en het vertrouwen in) het product niet altijd even duidelijk.

Een voorbeeld: Bij financiële schade door verloren persoonsgegevens bij het internetbankieren, kan een consument de betreffende bank aankijken (third party), de betreffende webshop (dienstenaanbieder), terwijl de fout wellicht ontstaan is door slechte beveiliging van de eigen pc (technologie). De deuk die het vertrouwen heeft opgelopen slaat daarmee wellicht terug op de verkeerde partij. Daarmee is de partij die het vertrouwen kan vergroten, ook niet automatisch de partij die het vertrouwen schade toebracht. Wanneer men uitspraken wil doen over het vertrouwen in specifieke producten of diensten met als doel om het vertrouwen te

verhogen, is het daarom belangrijk om de betrokken actoren in de analyse mee te nemen.

3 Aanpak

3.1 Monitoring framework Vertrouwen

Het monitoring framework om het vertrouwen in ICT-diensten verder in kaart te brengen zal gebaseerd zijn op het schema zoals gepresenteerd in hoofdstuk twee. In de komende paragrafen benoemen we kort de categorieën en indicatoren, de betrokken actoren en de methode voor waardebepaling.

3.1.1 Vertrouwenscategorieën en indicatoren

Zoals beschreven in hoofdstuk twee gaan we uit van zes dimensies van vertrouwen. In onderstaande tabel zijn de vertrouwensdimensies toegelicht en uitgewerkt naar indicatoren.

Vertrouwensdimensie	Betreft	Indicatoren
Sociaal	Sociale factoren met invloed op vertrouwen	Ervaring, bekendheid, groepsdruk, cultuur, normen en waarden.
Institutioneel	'Third parties' en institutionele context met invloed op vertrouwen	Reputatie, accreditatie (trustmarks), regelgeving, wettelijke verplichtingen.
Inhoud (*Information content)*	(Uiterlijke) Kenmerken van het product of de content met invloed op vertrouwen	Design, aanpassingsmogelijkheden (personificatie), merk zichtbaarheid.
Product	Product kenmerken die de aankoop/gebruiksbeslissing beïnvloeden	Beschikbaarheid, kwaliteit, duurzaamheid, prijs
Transactie	Kenmerken die het vertrouwen in de transactie vergroten.	Transparantie, betalingsmogelijkheden, afrekenmodel, kortingen.
Technologie	Kenmerken van infrastructuur en software die de effectiviteit en veiligheid beïnvloeden.	Veiligheid, integriteit, authenticiteit, vertrouwelijkheid, betrouwbaarheid.

De indicatoren in deze tabel hebben invloed op de vertrouwensdimensie waar zij toe behoren en daarmee tot het totale vertrouwen in een product of dienst. Belangrijk om op te merken is dat het bij de vertrouwensindicatoren in alle gevallen gaat om de perceptie van de gebruiker. We kunnen dus wel de verwachting uitspreken dat het vertrouwen in de technologie beïnvloed wordt door de gepercipieerde veiligheid of betrouwbaarheid van het product of dienst.
De indicatoren zoals benoemd in deze tabel, verschillen in hun mate van uitwerking. Om de invloed van culturele achtergrond op de sociale vertrouwensdimensie te bepalen, zullen meerdere subindicatoren moeten worden opgesteld. Dit geldt ook voor indicatoren als 'design' en 'regelgeving'. Sommige indicatoren zijn eenduidiger, zoals 'beschikbaarheid' en 'reputatie'.

Om te komen tot een inschatting van het vertrouwen, per dimensie of in zijn geheel, zal per dienst of product moeten worden bepaald welke indicatoren mee worden genomen in het onderzoek en hoe deze geoperationaliseerd worden. Hierbij is het van belang om mee te nemen welke dienstcomponenten en actoren een rol spelen.

3.1.2 Onderscheid in dienstcomponenten en actoren

De mate van vertrouwen in de technologie van een dienst is volgens bovenstaande tabel afhankelijk van kenmerken van de infrastructuur en software die de effectiviteit en veiligheid beïnvloeden.

Bij het gebruik van ICT-diensten spelen, zoals beschreven in paragraaf 2.2, verschillende actoren een rol. Per actor kan het vertrouwen in specifieke dimensies of in het totale product of dienst anders worden beïnvloed, wat het kwantificeren van vertrouwen lastig maakt.

Bij de meeste ICT-diensten zijn meerdere actoren betrokken. Vertrouwen in een actor heeft bijvoorbeeld te maken met reputatie en accreditatie en krijgt daarmee een plek in de institutionele dimensie. Toch spelen ook andere dimensies hier een rol. Een gebrek aan vertrouwen in de technologie, kan terugslaan op het vertrouwen in de actor die voor deze technologie verantwoordelijk is.

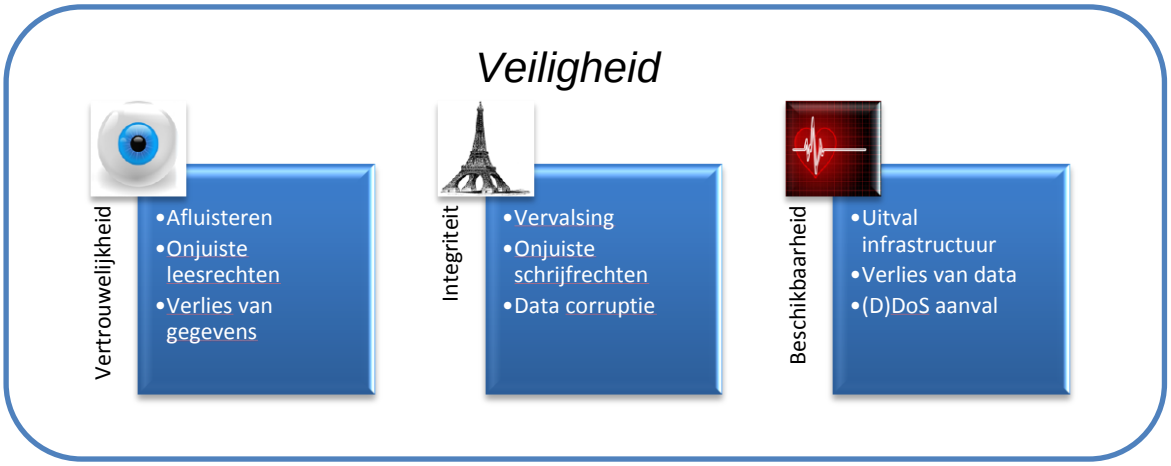
Dit hoeft echter niet altijd het geval te zijn: soms is het voor de gebruiker niet zichtbaar wie de technologie beheert, bijvoorbeeld door de vervlechting van verschillende componenten binnen een dienst (device, software, netwerk, third party), en zal de veiligheidsinschatting los staan van de betreffende actor.

3.1.3 Waardebepaling van indicatoren

In dit onderzoek zullen we geen waardebepaling toevoegen aan de resultaten die voor verschillende dimensies gevonden zijn. Dit wil zeggen dat er geen uitspraken worden gedaan of het vertrouwen (te) groot of (te) klein is. Dit komt omdat er gebruik wordt gemaakt van deskresearch. De diversiteit in onderzoeksmethoden, maakt de resultaten moeilijk onderling vergelijkbaar. In een wederkerend gebruikersonderzoek is dit wel mogelijk.

3.2 Monitoring framework Feiten

Het vertrouwen in ICT wordt deels bepaald door de Technologie-dimensie, waarvan veiligheid de voornaamste factor is. Veiligheid (informatiebeveiliging) bestaat uit een aantal categorieën, waaronder allerlei concrete feiten kunnen worden onderverdeeld.



3.2.1 *Beveiligingscategorieën en indicatoren*

Het vertrouwen in ICT wordt dus onder andere beïnvloed door problemen op het gebied van (informatie-) beveiliging. Dreigingen op dat vlak kunnen variëren van botnets en virussen tot identiteits- en creditcardfraude.

Informatiebeveiliging wordt standaard onderverdeeld in de volgende drie beveiligingscategorieën:

- Beschikbaarheid
- Integriteit
- Vertrouwelijkheid

Om in het monitoring framework een gestructureerd beeld te creëren, groeperen we alle problemen die een impact kunnen hebben op het vertrouwen in deze drie beveiligingscategorieën.

Voorbeelden van indicatoren per beveiligingscategorie zijn:

Beschikbaarheid - Is de dienst te gebruiken?
Oorzaken van beschikbaarheidsproblemen zijn onder andere storingen, performanceproblemen, en zogenaamde Denial-of-Service aanvallen.

Integriteit - Is de informatie correct?
Informatie kan corrupt raken door bijvoorbeeld storingen tijdens communicatie, corruptie van data-dragers, en wijziging van gegevens door aanvallers.

Vertrouwelijkheid - Is gevoelige informatie inzichtelijk voor ongeautoriseerde personen?

Voorbeelden zijn personeel dat klantinformatie verliest, aanvallers die gegevens buitmaken na een computerinbraak, en informatie over gebruikers van een dienst die zonder toestemming van de gebruiker wordt doorverkocht aan andere partijen.

3.2.2 Onderscheid in dienstcomponenten en actoren

Per categorie wordt onderscheid gemaakt in een aantal basiscomponenten van ICT, namelijk:

- Data
- Software
- Hardware
- Infrastructuur

Naast deze basiscomponenten zijn er nog twee eigenschappen die van groot belang zijn voor het vertrouwen in een ICT dienst:

- De afzetmarkt van de dienst
- Het goed verlopen van de financiële afhandeling

Informatie over de afname van de dienst kan van belang zijn voor het vertrouwen van aanbieder, bijvoorbeeld in het geval van wetgeving die afname verbiedt of ontmoedigd (denk aan kansspel-websites).

ICT, en dan met name ICT-dienstverlening, bestaat uit meerdere partijen. De aanbieder van een dienst (een ondernemer), de afnemer van de dienst (een consument), en eventueel andere ondersteunende partijen zoals transporteurs en payment providers.

De invloed op het vertrouwen van feiten is sterk afhankelijk van de partij die de risico's loopt. Om deze reden wordt voor de feiten een onderscheid gemaakt in consumenten en leveranciers. Ondersteunende partijen zijn niet expliciet meegenomen, maar zij kunnen in specifieke cases als leverancier fungeren.

3.2.3 Waardebepaling van feiten

Om de feiten te kunnen duiden is het wenselijk om per feit een score te hebben. Er is daarom gekozen om per feit een relatie te leggen met de situatie in andere (EU) landen.

Waar mogelijk wordt ook aangegeven wat het feit-niveau is voor:

- Europees gemiddelde
- Eurozone gemiddelde
- België
- Duitsland
- Verenigd koninkrijk

Hiermee wordt het mogelijk om een vergelijking te maken van de situatie in Nederland met omringende landen.

3.3 Dataverzameling

In dit onderzoek zijn data verzameld over de indicatoren op basis van deskresearch. Daarbij is gebruik gemaakt van zowel nationale als internationale studies en data.

4 Veiligheid

In dit hoofdstuk bespreken we de gevonden resultaten op basis van de indicatoren die eerder zijn geformuleerd.

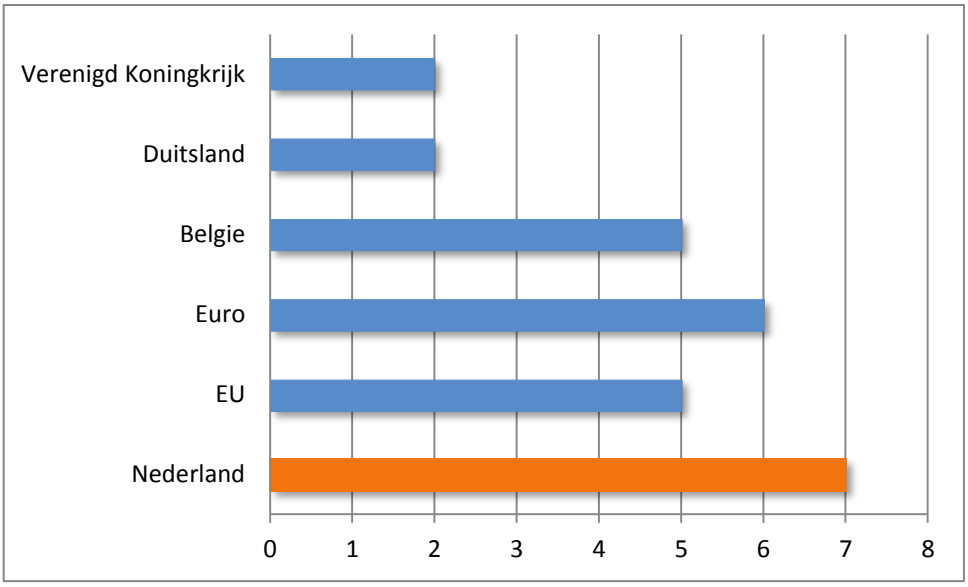
De feiten zijn opgesplitst in feiten die het algemene vertrouwen in ICT beïnvloeden, en feiten die het vertrouwen in e-Commerce beïnvloeden. Daarnaast wordt er (waar mogelijk) onderscheid gemaakt in de beveiligingscategorieën Beschikbaarheid, Integriteit en Vertrouwelijkheid. Als een feit te relateren is aan meerdere categorieën (bijvoorbeeld iets wat zowel impact kan hebben op de integriteit als de vertrouwelijkheid van informatie) is deze opgenomen in de eerste relevante categorie. Feiten die niet direct aan informatiebeveiliging te koppelen zijn, zijn verzameld onder de categorie Overig.

In de afsluitende paragraaf wordt een overzicht gepresenteerd van de gevonden informatie.

4.1 Algemeen – Beschikbaarheid

4.1.1 Incidenten bedrijven

Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij informatie vernietigd of gecorrumpeerd is, bedraagt 7% (zie Grafiek 1).

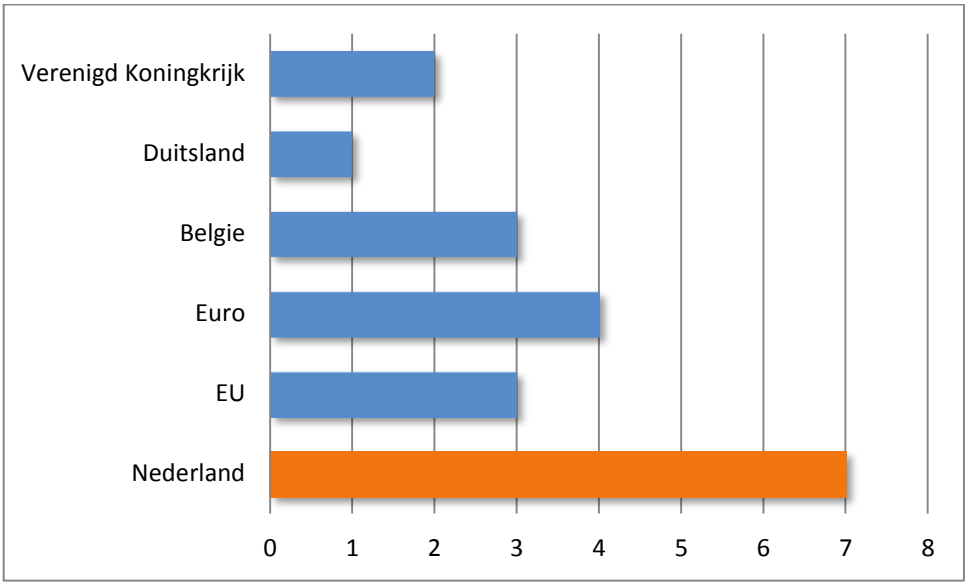


Grafiek 1 – Incidenten bedrijven 1 Bron: Eurostat

Daarmee scoort Nederland hoger dan het gemiddelde van de EU (5%) en de Eurozone (6%). Hoewel Duitsland en Engeland minder incidenten ondervonden, is het Nederlandse beeld vergelijkbaar met het gemiddelde beeld in Europa.

Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij ICT dienstverlening is verstoord door externe aanvallen, bedraagt 7% (Zie Grafiek 2).

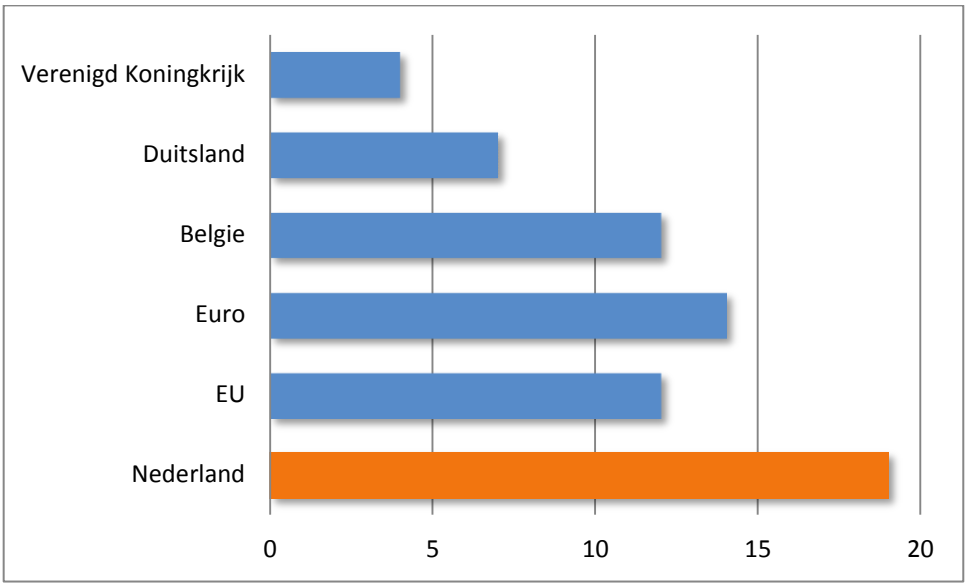
Hierbij gaat het bijvoorbeeld om (D)DoS aanvallen op de systemen of netwerkverbindingen van een bedrijf.



Grafiek 2 – Incidenten bedrijven 2 Bron: Eurostat

Nederland scoort hierbij wat slechter dan gemiddeld. Duidelijk is dat omringende landen minder last hebben van aanvallen. Een mogelijke oorzaak kan zijn dat Nederlandse bedrijven meer gebruik maken van ICT dan deze landen en daardoor meer risico lopen.

Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij ICT dienstverlening is verstoord door hardware- of software-problemen, bedraagt 19% (zie Grafiek 3).

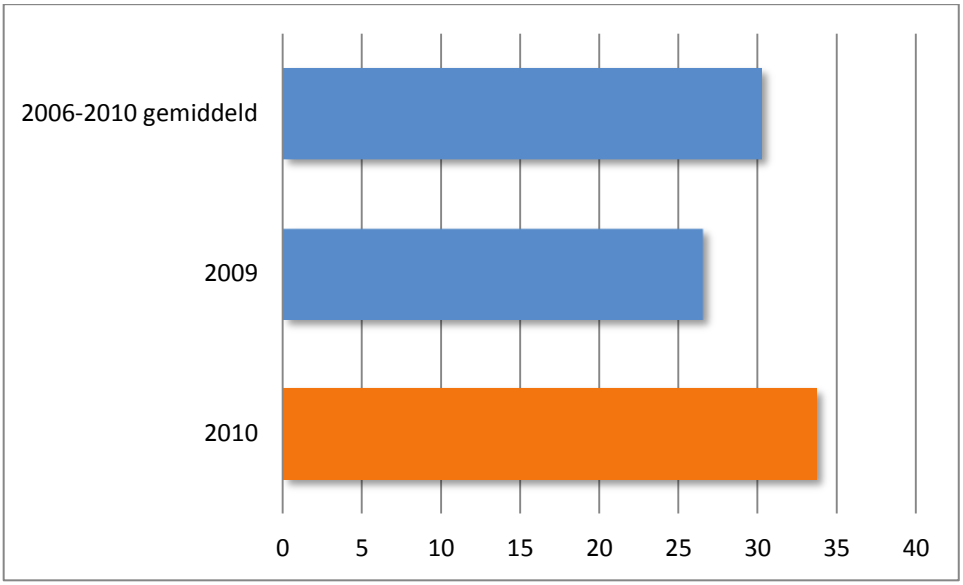


Grafiek 3 – Incidenten bedrijven 3 Bron: Eurostat

Ook hier scoort Nederland veel slechter dan haar buurlanden, mogelijk door een intensiever gebruik van ICT door het bedrijfsleven.

4.1.2 Stroomuitval

De gemiddelde tijdsduur dat huishoudens in Nederland in 2010 geen elektriciteit geleverd kregen, bedraagt 33,7 minuten (Zie Grafiek 4).



Grafiek 4 – Stroomuitval Bron: Energiened.nl

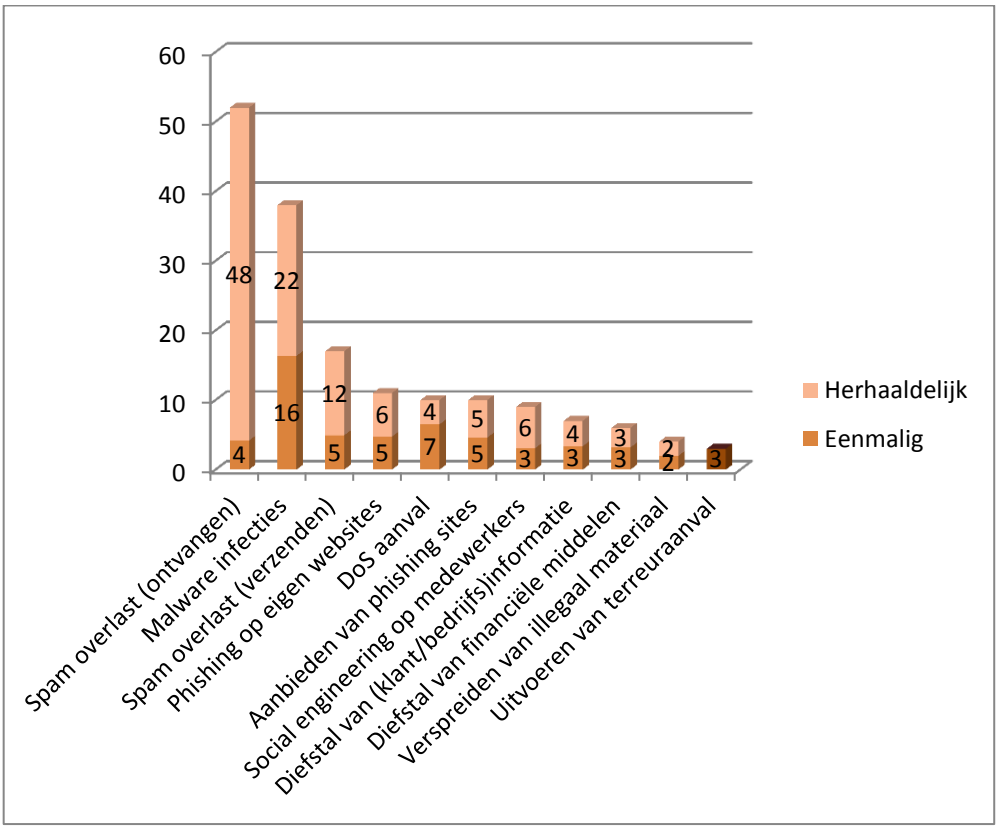
De beschikbaarheid van de stroomvoorziening wijkt daarmee niet significant af ten opzichte van de voorgaande jaren.

4.2 Algemeen – Integriteit

4.2.1 Cybercrime bij bedrijven

Het percentage Nederlandse bedrijven dat in 2010 te maken had met infectie van computersystemen van de organisatie door malware, bedraagt 38%. (Bron: ICT Barometer over Cybercrime 2011, E&Y)

In Grafiek 5 is weergegeven wat de frequentie is van de meest voorkomende cybercrime incidenten.

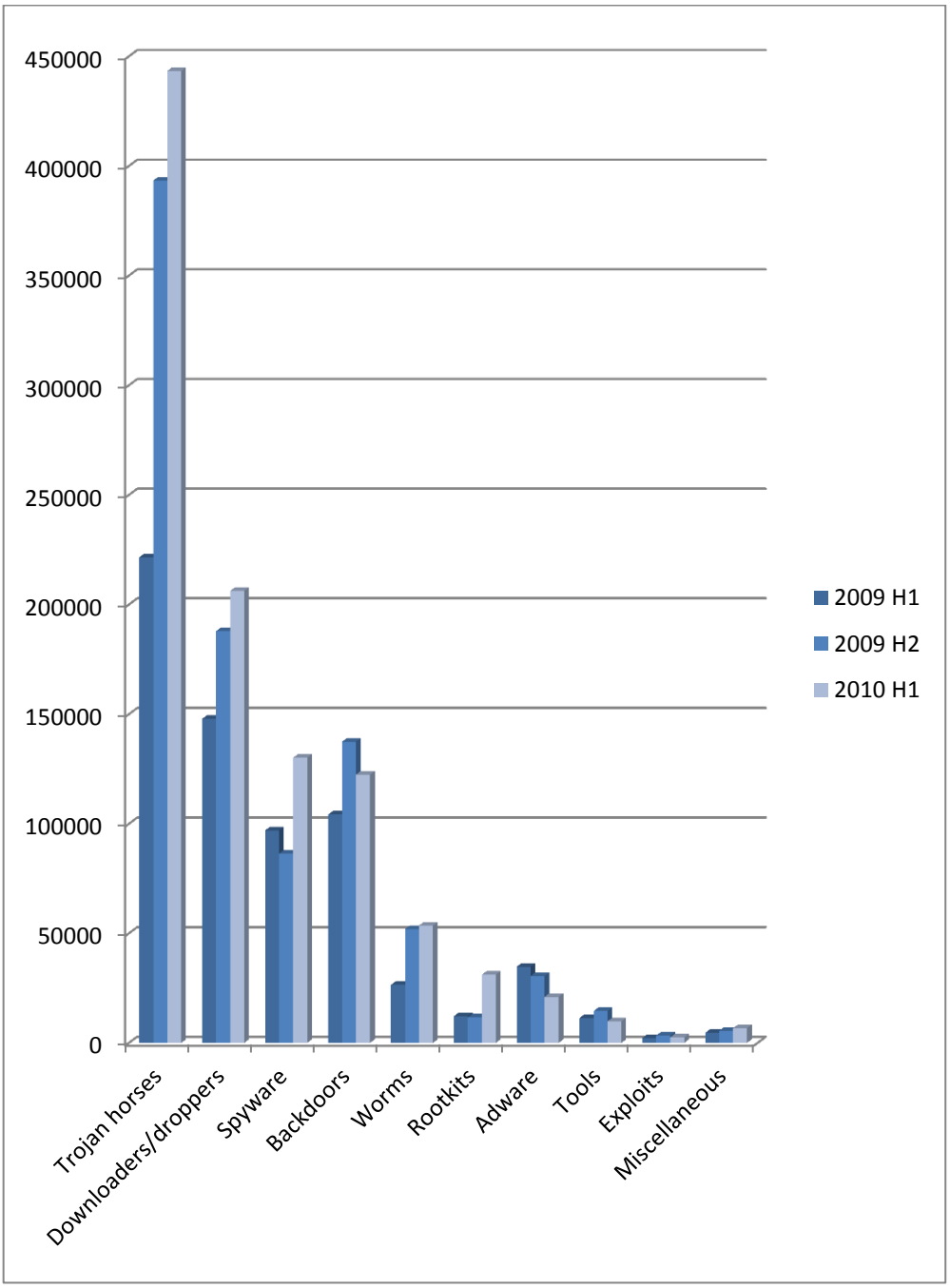


Grafiek 5 – Cybercrime bij bedrijven Bron: ICT Barometer Cybercrime.

Cijfers over het (via computersystemen) uitvoeren van een terreuraanval zijn niet nader uitgesplitst in percentages van bedrijven die er eenmalig of herhaaldelijk last van hebben ondervonden.

Duidelijk is dat het ontvangen van Spam-berichten en malware infecties tot de meest voorkomende type cybercrime incidenten behoren. Er zijn geen cijfers bekend over de voorgaande jaren.

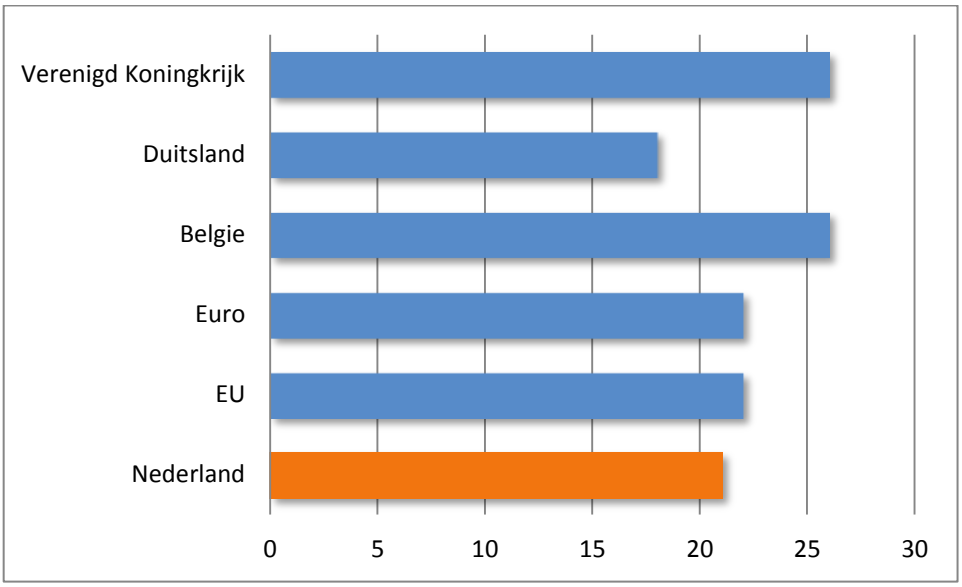
Informatie over malware die inzicht biedt in het verloop in de tijd kan deels uit de statistieken van antivirusbedrijf G-Data gehaald worden (zie Grafiek 6).



Grafiek 6 – Malware detectie door G-Data Bron: G-Data

4.2.2 *Security incidenten bij particulieren*

Het percentage Nederlanders dat in 2010 door internetgebruik een geïnfecteerde computer heeft opgelopen, bedraagt 21% (zie Grafiek 7).



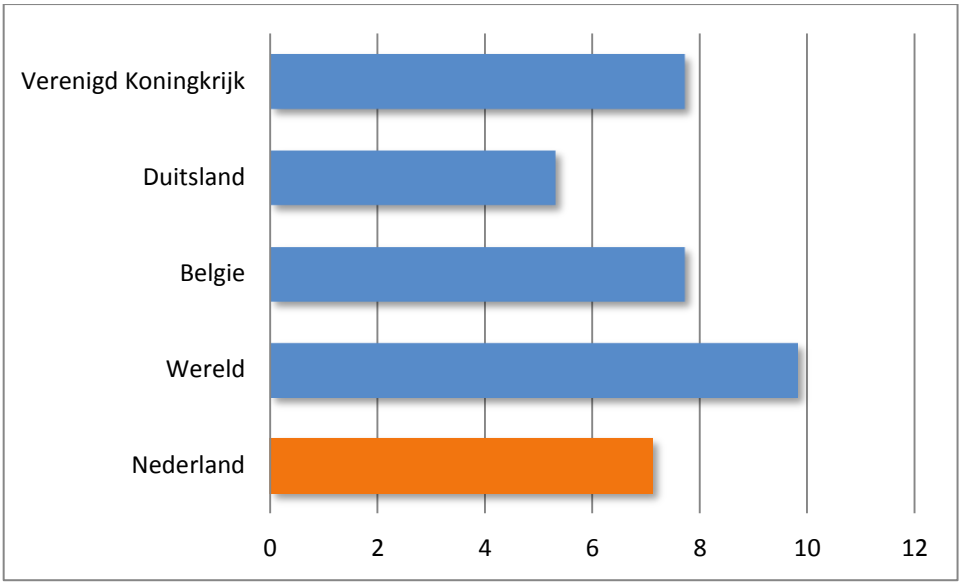
Grafiek 7 – Malware-infectie particulieren Bron: Eurostat

Eén op de vijf Nederlanders heeft in 2010 dus, via Internet, een malware-besmetting opgelopen op hun computer. Deze verhouding is ook te zien in de meeste andere landen uit de Eurozone, hoewel mensen uit België en het Verenigd Koninkrijk duidelijk meer last hebben gehad.

Cijfers over besmetting via andere bronnen, bijv. via USB-stick/CD-ROM of e-mail, zijn niet bekend.

4.2.3 Botnet-besmetting en Spam

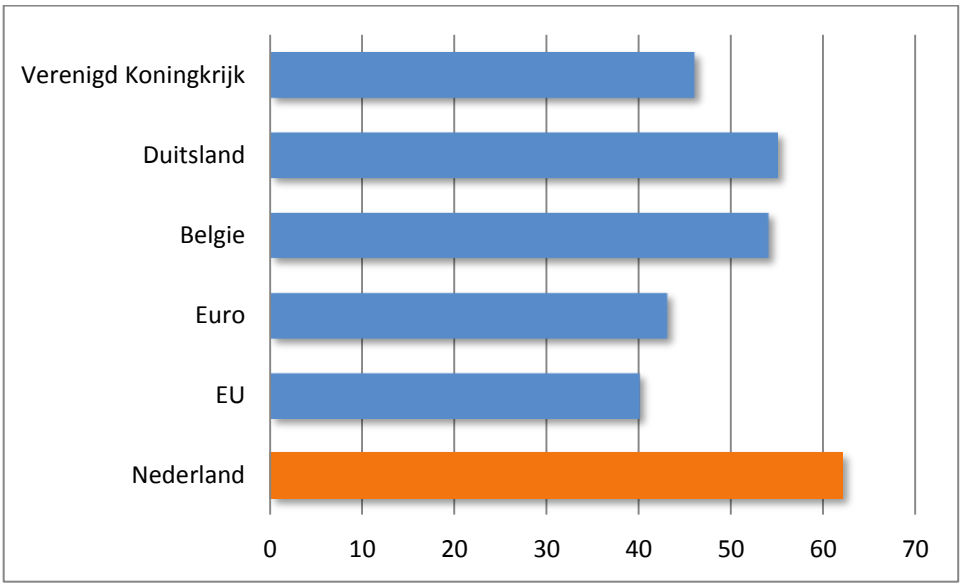
Het gemiddeld aantal met botnet-malware besmette Nederlandse computers per 1000 uitvoeringen van de Microsoft Malicious Software Removal Tool in 2010, bedraagt 7,1 (zie Grafiek 8).



Grafiek 8 – Botnet-besmetting Bron: Microsoft Intelligence Report

Qua botnet besmettingen doet Nederland het gemiddeld. Het is lastig om te vergelijken met andere landen, omdat botnet-besmettingen vaak regionaal plaatsvinden – als er bijvoorbeeld een Nederlandstalige email met malware-bijlage wordt verspreid zal dat tot veel besmettingen leiden in Nederland (en België) maar niet in Duitsland.

Het percentage Nederlanders dat in 2010 ongewenste emailberichten heeft ontvangen, bedraagt 62% (zie Grafiek 9).



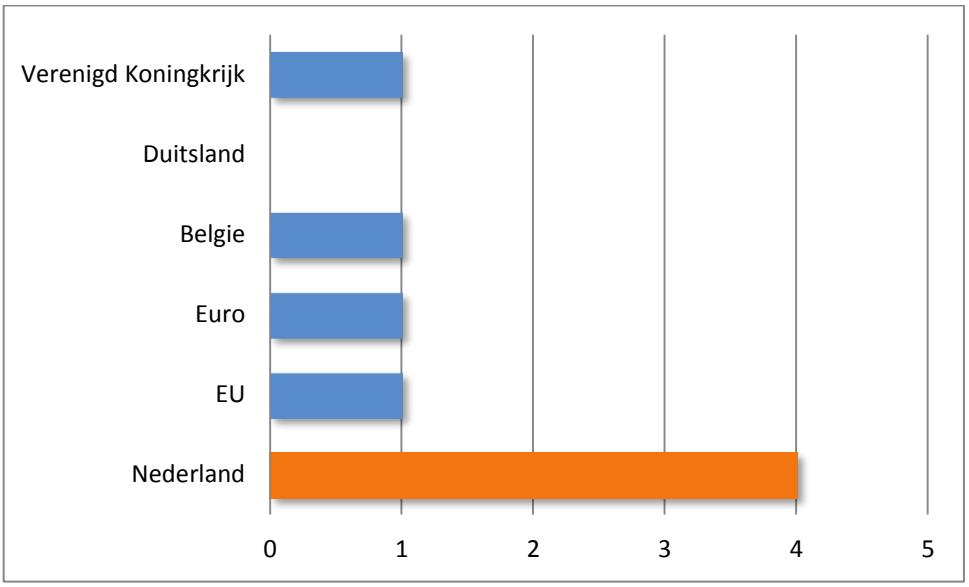
Grafiek 9 – Spam particulieren Bron: Eurostat

Met 62% scoort Nederland duidelijk slechter dan de meeste andere landen in Europa. Dit kan echter gerelateerd zijn aan het aantal mensen dat (regelmatig) gebruik maakt van email. Als wordt vergeleken met het Internetgebruik (zie Internetgebruik) valt op dat mensen uit het Verenigd Koninkrijk minder last hebben van spam dan op basis van Internetgebruik verwacht is.

4.3 Algemeen – Vertrouwelijkheid

4.3.1 Incidenten bedrijven

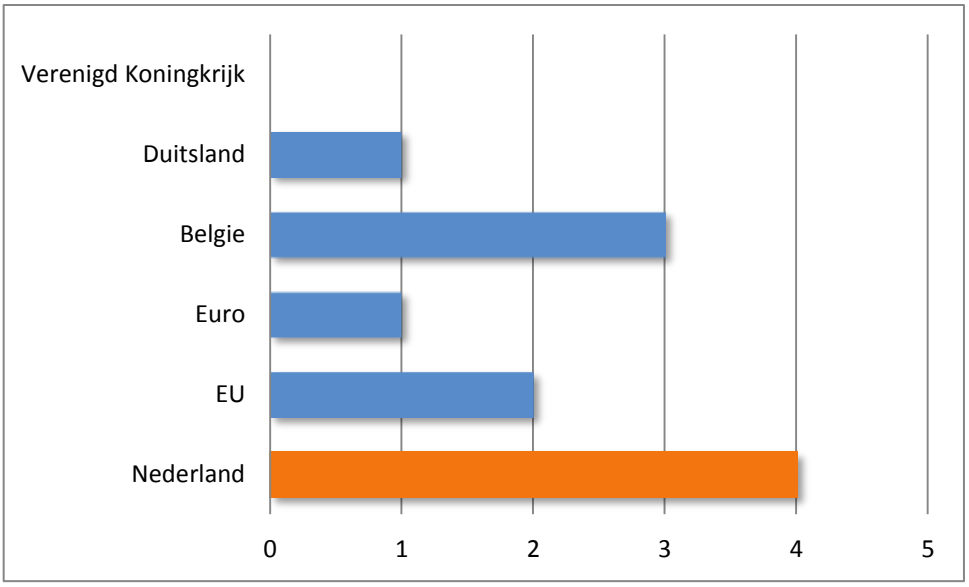
Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij gevoelige informatie is uitgelekt door middel van IT aanvallen, bedraagt 4% (zie Grafiek 10).



Grafiek 10 – Incidenten bedrijven 4 Bron: Eurostat

Nederland scoort hier significant slechter dan de rest van de EU. Alleen Slowakije heeft eenzelfde percentage van bedrijven – daaronder is de slechtste score 2%.

Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij (al dan niet opzettelijk) gevoelige informatie is uitgelekt door medewerkers, bedraagt 4% (zie Grafiek 11).

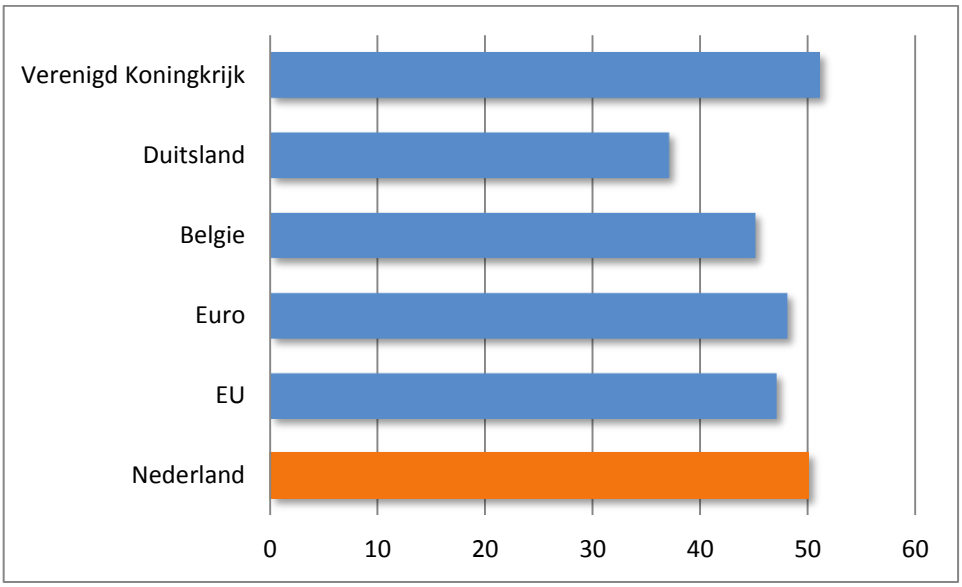


Grafiek 11 – Incidenten bedrijven 5 Bron: Eurostat

Cyprus (met 21%) en Slowakije (6%) zijn de enige landen in de EU met een slechtere score. De situatie in Nederland lijkt echter niet significant af te wijken van die in België. Voor het Verenigd Koninkrijk is geen informatie beschikbaar.

4.3.2 Wachtwoordsterkte bedrijven

Het percentage van Nederlandse bedrijven, exclusief de financiële sector, die in 2010 sterke wachtwoorden toepasten (min. 8 karakters, max. 6 maanden geldig, vercijferd transport en opslag), bedraagt 50% (zie Grafiek 12).



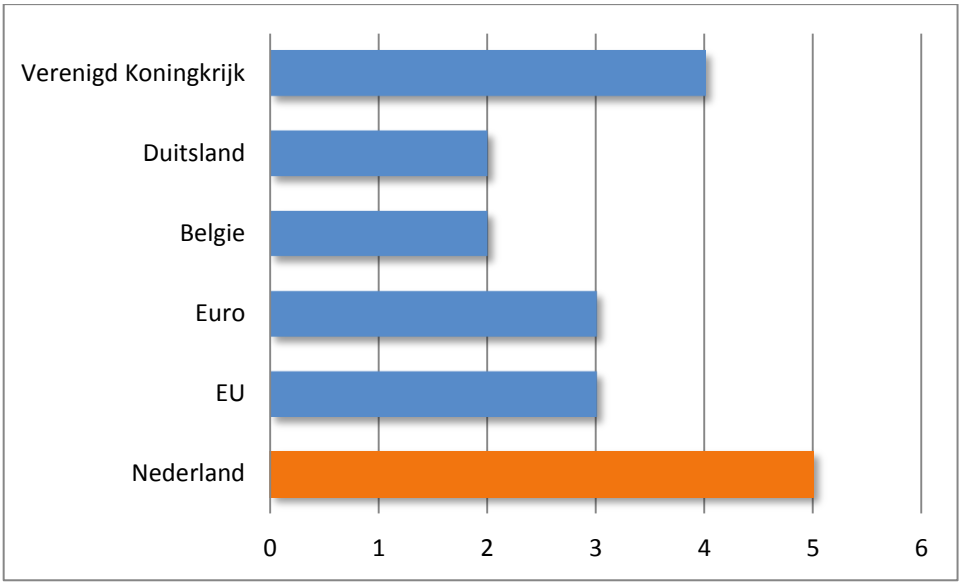
Grafiek 12 – Wachtwoordsterkte bedrijven Bron: Eurostat

Nederland doet het wat betreft wachtwoordsterkte wat beter dan de meeste andere Europese landen. Vooral met betrekking tot Duitsland is er een significant verschil.

4.4 Algemeen – Overig

4.4.1 Misbruik persoonlijke informatie

Het percentage Nederlanders dat in 2010 door internetgebruik te maken heeft gehad met misbruik van persoonlijke informatie (foto's, video's of persoonsgegevens die op community sites zijn geplaatst), bedraagt 5% (zie Grafiek 13).

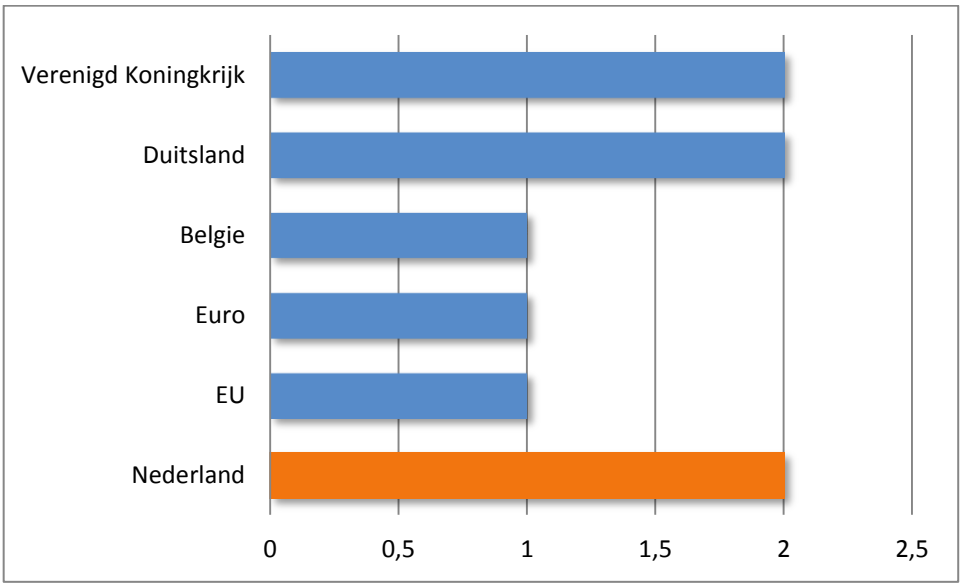


Grafiek 13 – Misbruik persoonlijke informatie Bron: Eurostat

Ook bij dit type incidenten scoort Nederland slechter dan het Europees gemiddelde.

4.4.2 *Phishing & pharming*

Het percentage Nederlanders dat in 2010 door internetgebruik financiële schade heeft ondervonden naar aanleiding van phishing of pharming, bedraagt 2% (zie Grafiek 14).

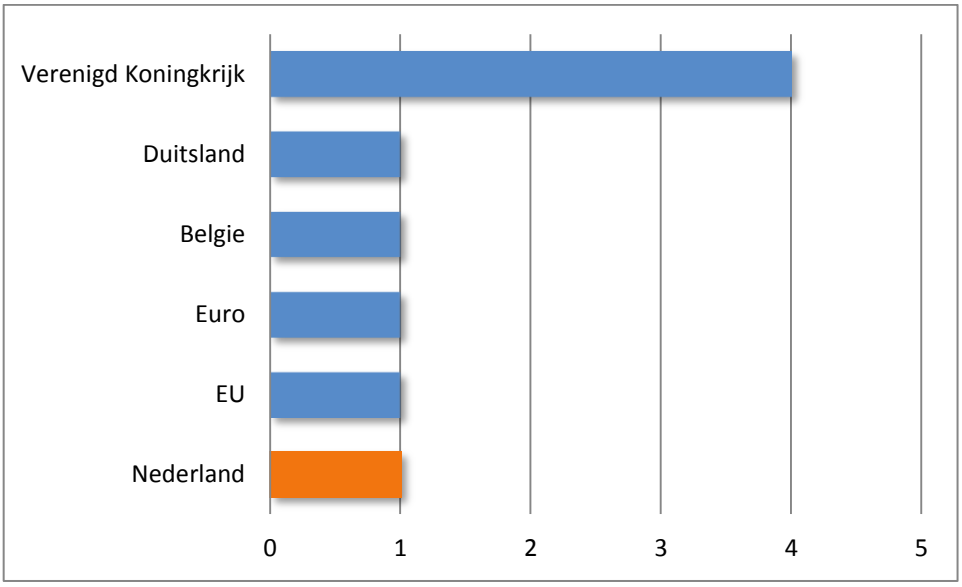


Grafiek 14 – Schade phishing pharming Bron: Eurostat

Het percentage mensen dat financiële schade heeft ondervonden door Internetgebruik is vergelijkbaar met de situatie in andere Eurozone landen.

4.4.3 Betaalkaartmisbruik

Het percentage Nederlanders dat in 2010 door internetgebruik financiële schade heeft ondervonden naar aanleiding van betaalkaartmisbruik, bedraagt 1% zie Grafiek 15).

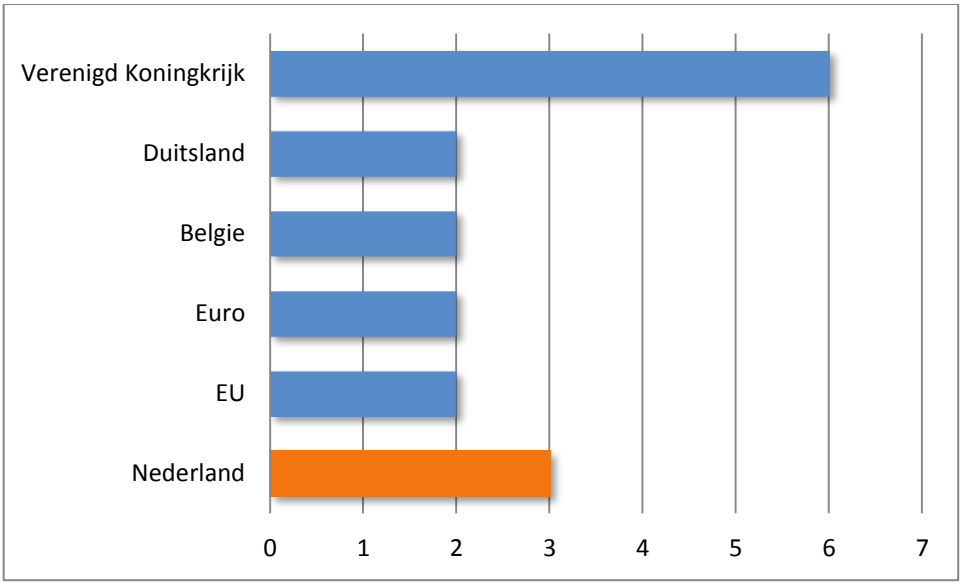


Grafiek 15 – Betaalkaartmisbruik Bron: Eurostat

In Nederland wordt, op een vergelijkbaar niveau van de meeste andere Europese landen, misbruik gemaakt van betaalkaarten. Het Verenigd Koninkrijk scoort echter een stuk slechter op dit vlak.

4.4.4 Financiële schade internetgebruik

Het percentage Nederlanders dat in 2010 door internetgebruik financiële schade heeft ondervonden (door willekeurige oorzaken), bedraagt 3% (zie Grafiek 16).

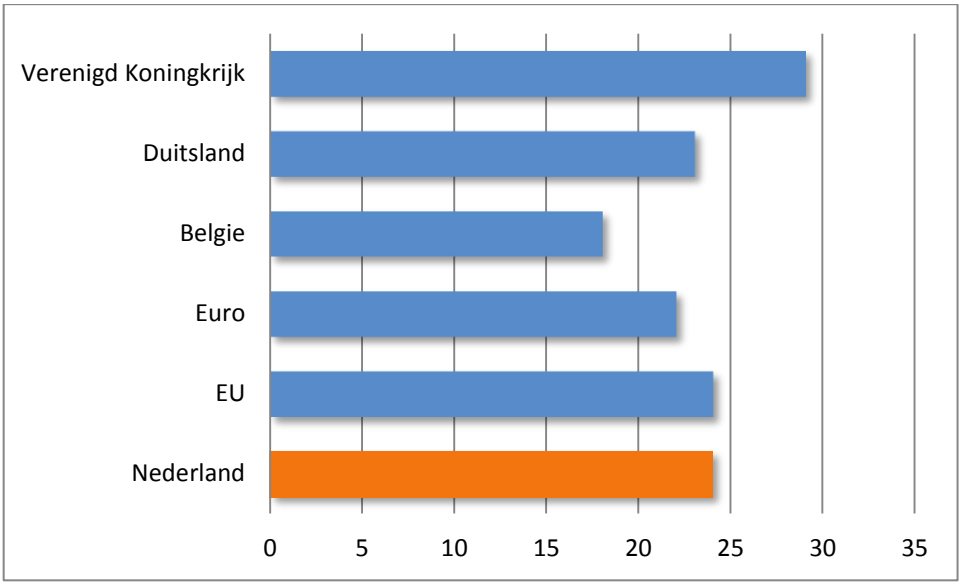


Grafiek 16 – Financiële schade internetgebruik Bron: Eurostat

Door Internetgebruik veroorzaakte financiële schade is in Nederland op een vergelijkbaar niveau als de rest van de Eurozone.

4.4.5 Geen beveiligingsproblemen

Het percentage Nederlanders dat in 2010 geen beveiligingsproblemen heeft ondervonden bij internetgebruik, bedraagt 24% (zie Grafiek 17).



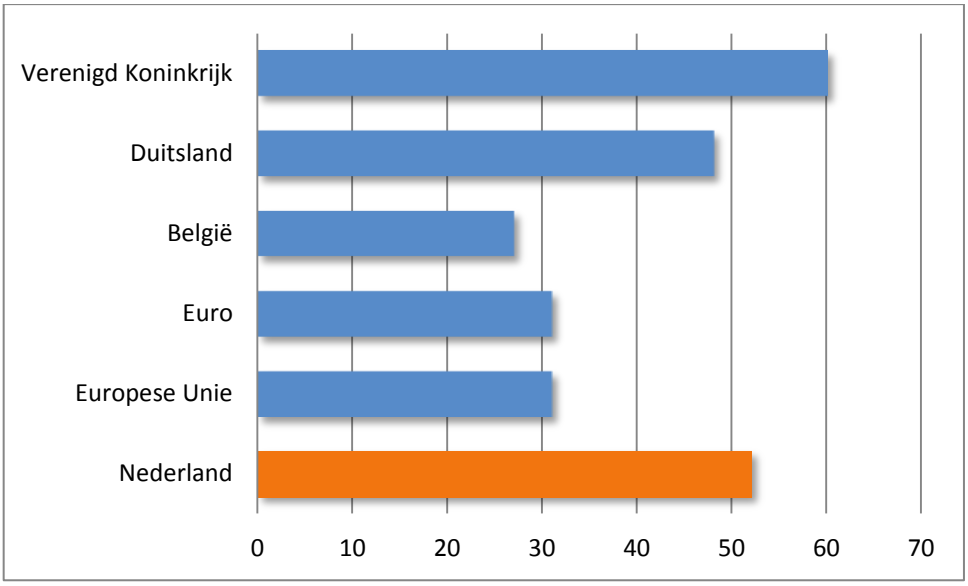
Grafiek 17 – Geen beveiligingsproblemen Bron: Eurostat

Nederland scoort wat dit betreft gemiddeld, Oostenrijk (52%) presteert het beste en de voormalige Joegoslavische republiek Macedonië het slechtste (7%).

4.5 E-Commerce – Overig

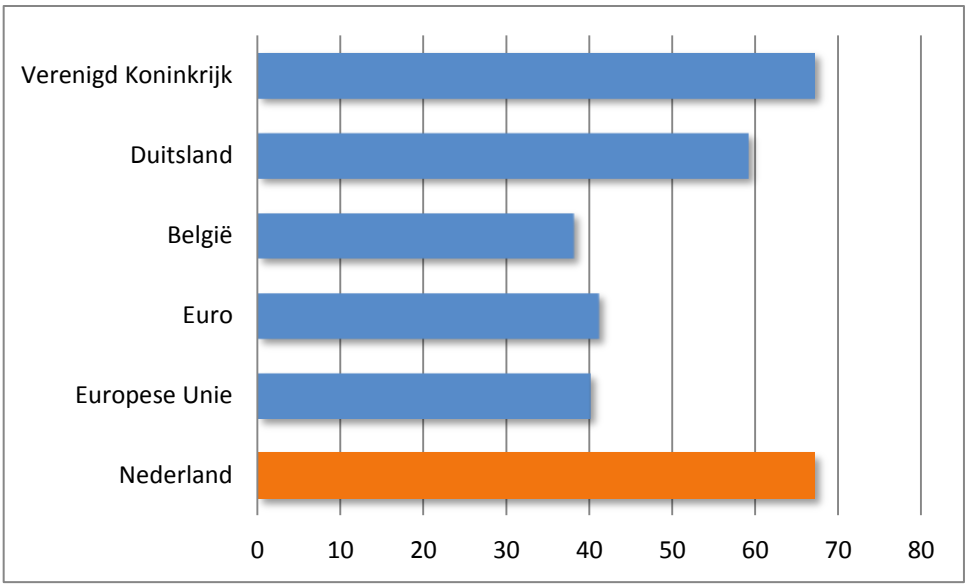
4.5.1 Aanschaf via Internet

Het percentage Nederlanders dat in 2010 in de voorgaande 3 maanden iets via Internet hebben aangeschaft, bedraagt 52% (zie Grafiek 18).



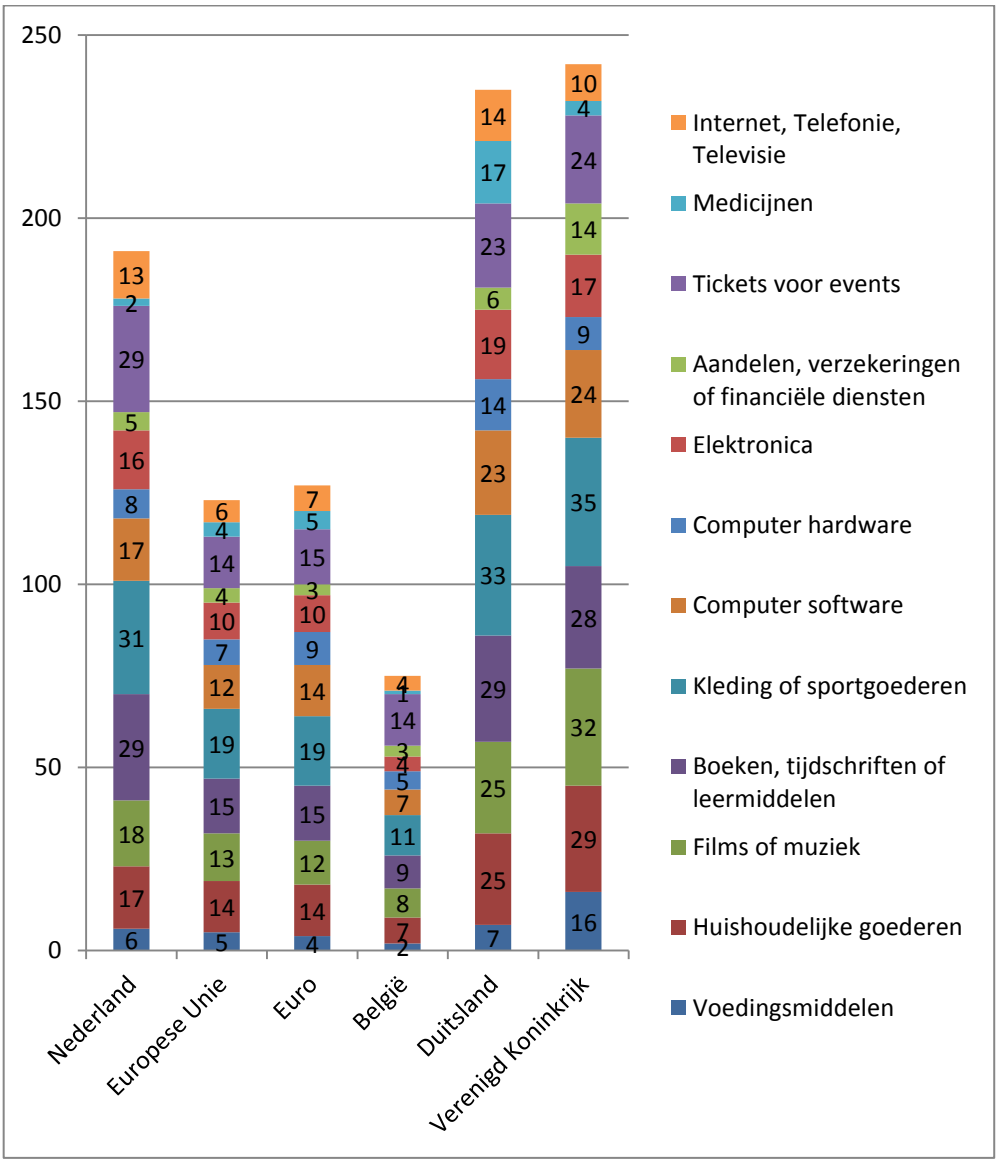
Grafiek 18 – Aanschaf via Internet 3 maanden Bron: Eurostat

Het percentage Nederlanders dat in 2010 in de afgelopen 12 maanden iets via Internet hebben aangeschaft, bedraagt 67% (zie Grafiek 19).



Grafiek 19 – Aanschaf via Internet 12 maanden Bron: Eurostat

In Grafiek 20 wordt weergegeven wat de aanschafpercentages zijn (gemeten over de afgelopen 12 maanden, in 2010) voor verschillende categorieën goederen/diensten. Ter illustratie: 29% van de Nederlanders hebben tickets voor events gekocht, 5% heeft aandelen e.d. gekocht, etc. Aangezien één persoon producten/diensten uit meerdere categorieën kan aanschaffen, kan het totaal per land boven de 100% uitkomen.



Grafiek 20 – Onderverdeling goederen/diensten Bron: Eurostat

4.6 Overzicht

In onderstaand overzicht zijn de feiten voor het jaar 2010 samengevat, die van invloed kunnen zijn op het vertrouwen van ICT dienst-aanbieders. De detailinformatie is in de voorgaande paragrafen te vinden.

De categorie kan B, I en/of V zijn, wat staat voor de beveiliging categorieën Beschikbaarheid, Integriteit en Veiligheid. Tot slot wordt aangegeven op welke dienstcomponent(en) het feit betrekking heeft.

Ondernemer	Consument	Categorie	Data	Software	Hardware	Infrastructuur	Gebruik	financiën	Feit	Waarde
Algemeen										
X		**B**	**X**						Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij informatie vernietigd of gecorrumpeerd is	7%
X		**B**		**X**		**X**			Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij ICT dienstverlening is verstoord door externe aanvallen	7%
X		**B**		**X**	**X**				Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij ICT dienstverlening is verstoord door hardware- of software-problemen	19%
X		**B**				**X**			De gemiddelde tijdsduur dat huishoudens in Nederland in 2010 geen elektriciteit geleverd kregen	34 min
X	**X**	**IV**	**X**	**X**					Het percentage Nederlandse bedrijven dat in 2010 te maken had met infectie van computersystemen van de organisatie door malware	38%
	X	**IV**	**X**	**X**					Het percentage Nederlanders dat in 2010 door internetgebruik een geïnfecteerde computer heeft opgelopen	21%
	X	**IV**	**X**	**X**					Het gemiddeld aantal met botnet-malware besmette Nederlandse computers per 1000 uitvoeringen van de Microsoft Malicious Software Removal Tool in 2010	7,1
	X	**I**	**X**						Het percentage Nederlanders dat in 2010 ongewenste emailberichten heeft ontvangen	62%
X		**V**	**X**						Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij gevoelige informatie is uitgelekt door middel van IT aanvallen	4%
X		**V**	**X**						Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij (al dan niet opzettelijk) gevoelige informatie is uitgelekt door medewerkers	4%
X	**X**	**V**		**X**					Het percentage van Nederlandse bedrijven, exclusief de financiële sector, die in 2010 sterke wachtwoorden toepasten (min. 8 karakters, max. 6 maanden geldig, vercijferd transport en opslag)	50%

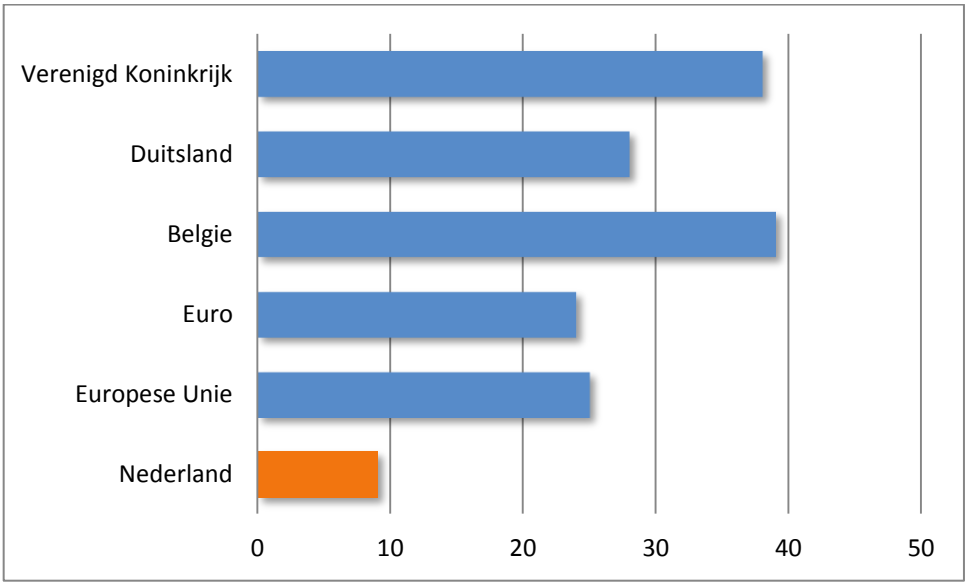
	X		**X**						Het percentage Nederlanders dat in 2010 door internetgebruik te maken heeft gehad met misbruik van persoonlijke informatie (foto's, video's of persoonsgegevens die op community sites zijn geplaatst)	5%
	X							**X**	Het percentage Nederlanders dat in 2010 door internetgebruik financiële schade heeft ondervonden naar aanleiding van phishing of pharming	2%
	X							**X**	Het percentage Nederlanders dat in 2010 door internetgebruik financiële schade heeft ondervonden naar aanleiding van betaalkaartmisbruik	1%
	X							**X**	Het percentage Nederlanders dat in 2010 door internetgebruik financiële schade heeft ondervonden (door willekeurige oorzaken)	3%
	X								Het percentage Nederlanders dat in 2010 geen beveiligingsproblemen heeft ondervonden bij internetgebruik	24%
e-Commerce specifiek										
X							**X**	**X**	Het percentage Nederlanders dat in 2010 in de voorgaande 3 maanden iets via Internet hebben aangeschaft	52%
X							**X**	**X**	Het percentage Nederlanders dat in 2010 in de afgelopen 12 maanden iets via Internet hebben aangeschaft	67%
X							**X**	**X**	Het percentage Nederlanders dat in 2010 medicijnen via het Internet heeft gekocht	2%
X							**X**	**X**	Het percentage Nederlanders dat in 2010 via het Internet telecomdiensten heeft aangeschaft (bijvoorbeeld het opwaarderen van telefoonkaarten, het afnemen van TV / Internet diensten)	13%

5 Vertrouwen

Dit hoofdstuk bespreekt de resultaten met betrekking tot vertrouwen.

5.1 Vertrouwen in ICT-diensten

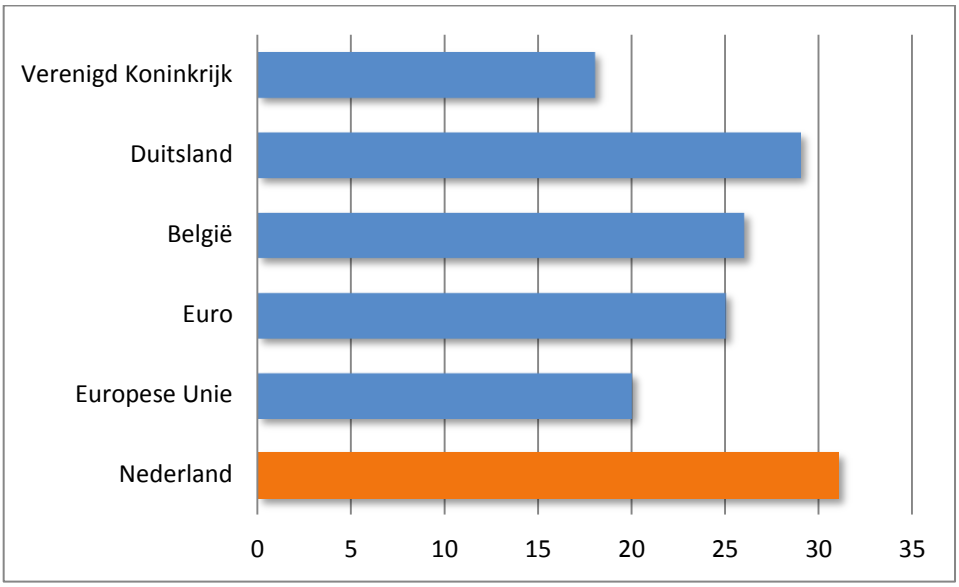
Het percentage individuen dat zich in 2010 ernstig zorgen maakt over het opdoen van virussen bij het gebruik van internet, wat kan resulteren in dataverlies, bedraagt 9%.



Grafiek 21 – Zeer bezorgd om virussen via Internet Bron: Eurostat

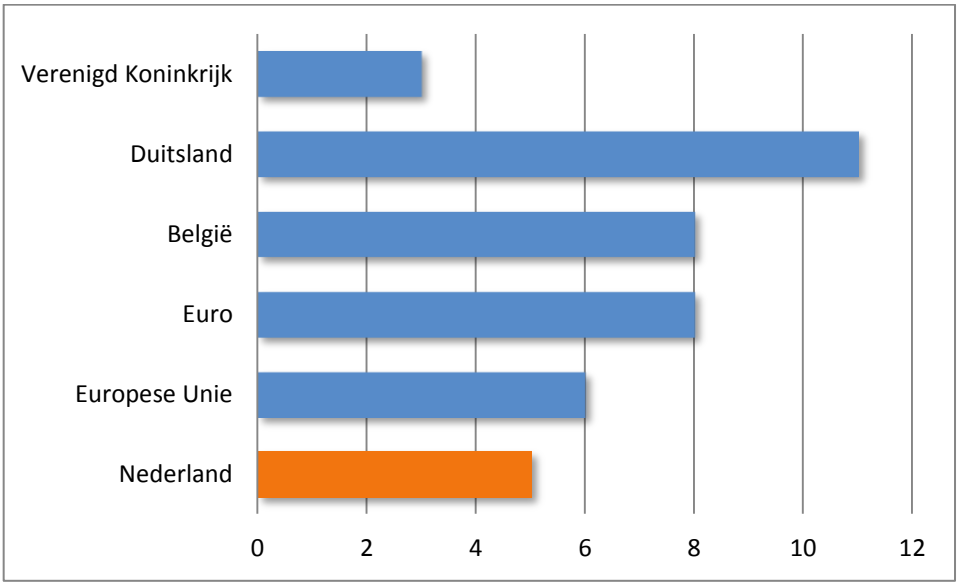
Nederlanders maken zich, in verhouding tot andere Europese landen, relatief weinig zorgen over het opdoen van virussen bij het internet gebruik. Negen procent zegt zich hier wel eens zorgen over te maken. Gemiddeld ligt dit percentage op 25%. Het Verenigd Koninkrijk en België scoren nog hoger met respectievelijk 38% en 39%.

Nederlanders maken zich meer zorgen dan omliggende landen over de veiligheid van hun persoonlijke gegevens op online sociale netwerken. Bijna een derde (31%) van de Nederlanders geeft aan uit veiligheidsoverweging geen persoonlijke informatie via deze platforms te delen (zie Grafiek 22).



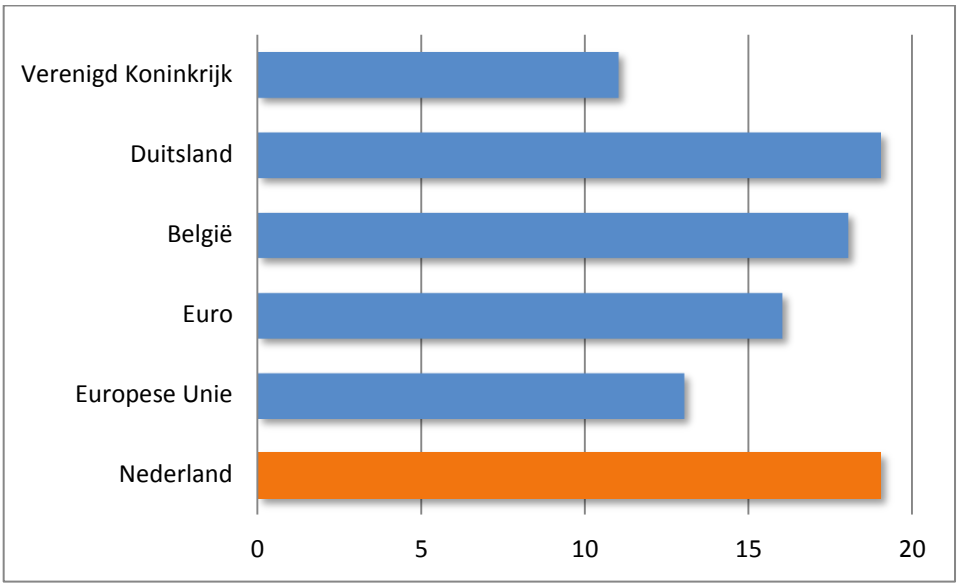
Grafiek 22 – Persoonlijke informatie community sites Bron: Eurostat

In de publieke dienstverlening via ICT-middelen heeft de Nederlander meer vertrouwen. Vijf procent van de Nederlanders maakt liever geen gebruik van publieke diensten of administraties via de computer. Dit percentage ligt iets onder het Europees gemiddelde (zie grafiek 23).



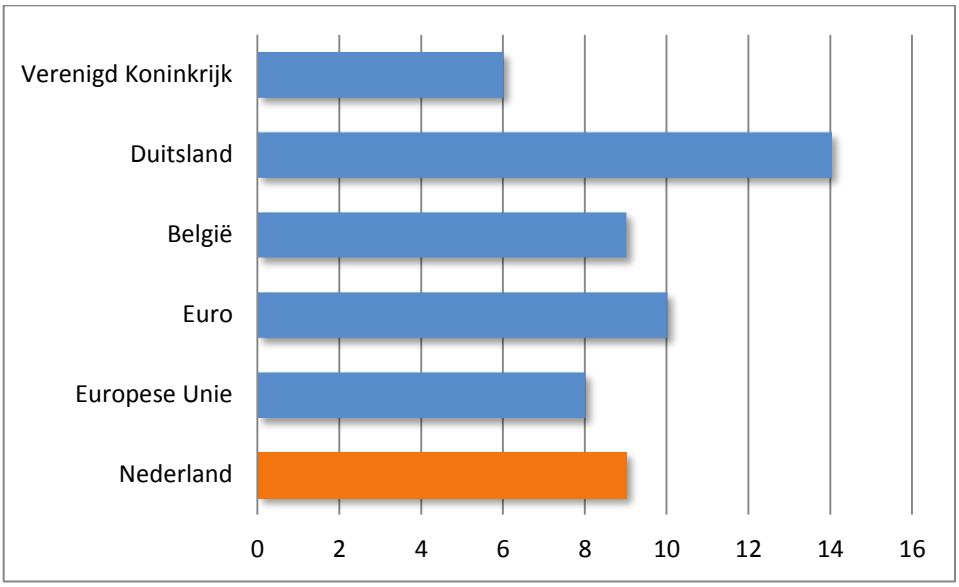
Grafiek 23 – Geen communicatie met publieke diensten/administraties Bron: Eurostat

Bijna een op de vijf Nederlanders mijdt het downloaden van muziek, games of films via internet vanwege veiligheidsredenen (zie grafiek 24). Daarin zijn we net zo terughoudend als onze oosterburen, maar scoren we wel enkele procentpunten hoger dan het Europees gemiddelde.



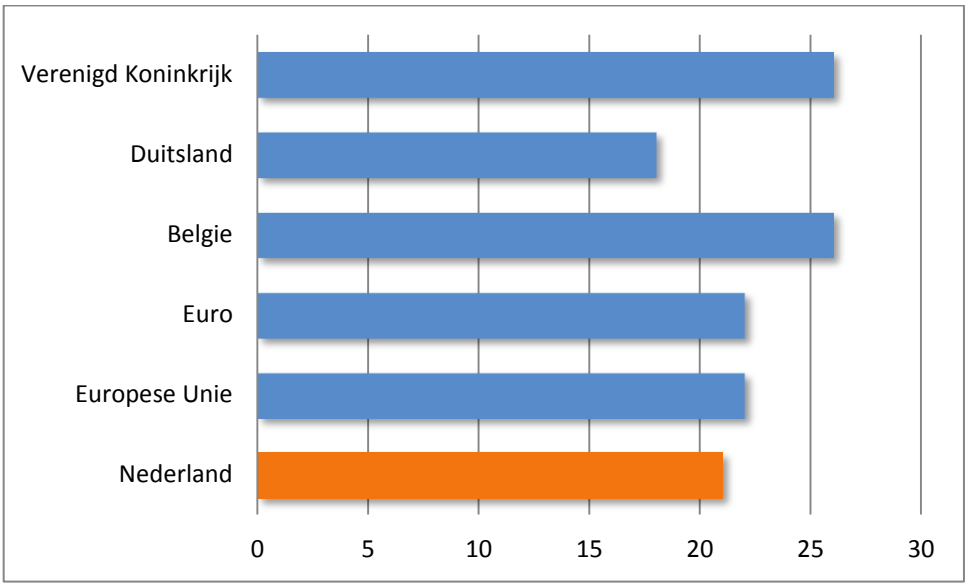
Grafiek 24 – Geen download van informatie via Internet Bron: Eurostat

Steeds vaker maken we gebruik van draadloze netwerken. In steeds meer ruimtes wordt in deze verbindingen voorzien. Negen procent van de Nederlanders maakt uit veiligheidsoverweging geen gebruik van deze ‘vreemde’ verbindingen. Daarmee wijkt Nederland weinig af van de gemiddelde score in de Europese Unie (zie grafiek 25).



Grafiek 25 - Geen gebruik van Internet via vreemde draadloze netwerken Bron: Eurostat

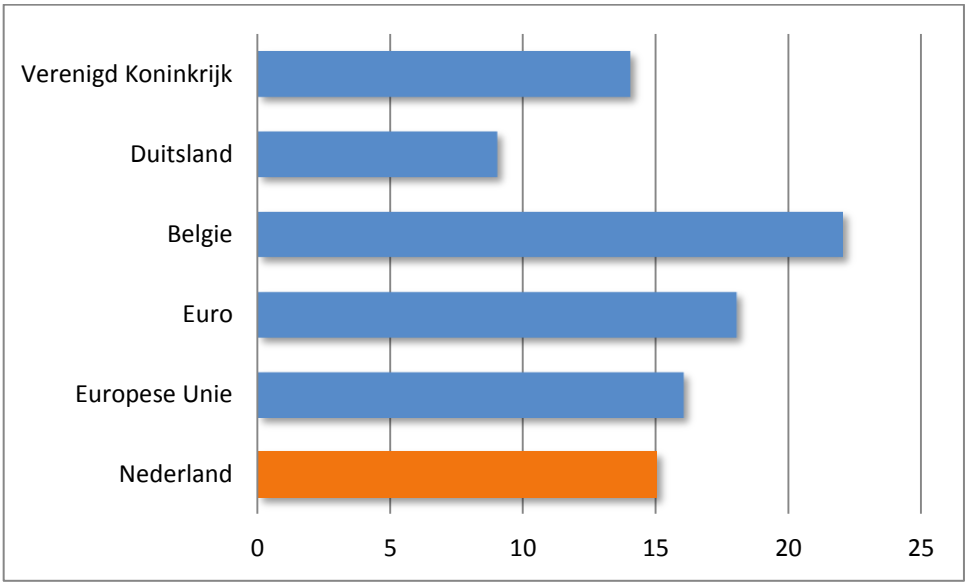
In 2010 ondervond iets meer dan een op de vijf Nederlanders wel eens hinder van veiligheidsgerelateerde problemen bij het gebruik van internet. Dit ligt dicht bij het Europees gemiddelde van 22 procent. In België en Duitsland worden vaker problemen ervaren door internetgebruikers (zie grafiek 26).



Grafiek 26 – Veiligheidsproblemen bij Internetgebruik Bron: Eurostat

5.2 Vertrouwen in e-Commerce

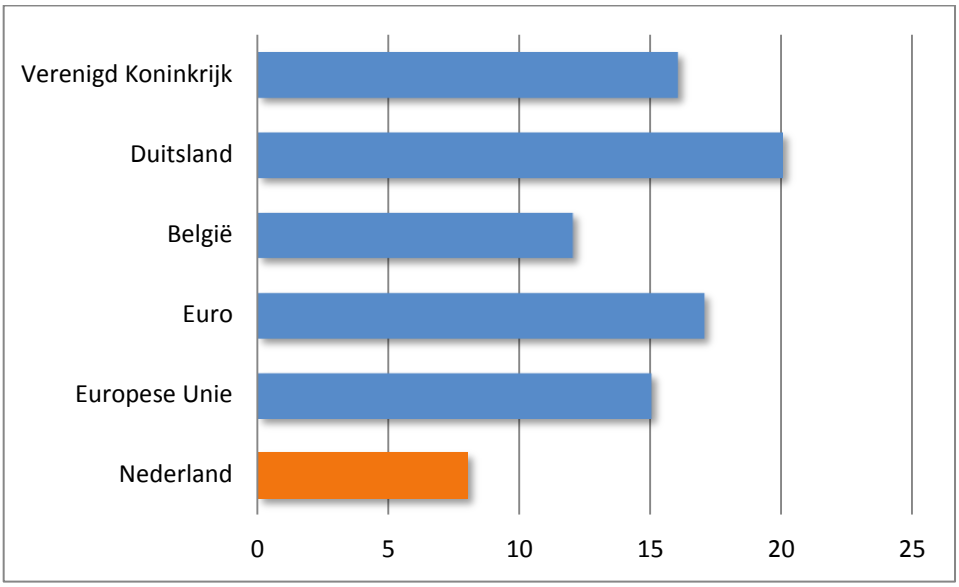
Het percentage individuen dat uit veiligheidsoverwegingen af zag van het bestellen of aankopen van goederen of diensten voor persoonlijk gebruik, bedraagt 15%.



Grafiek 27 – Afzien bestel/aanschaf goederen Bron: Eurostat

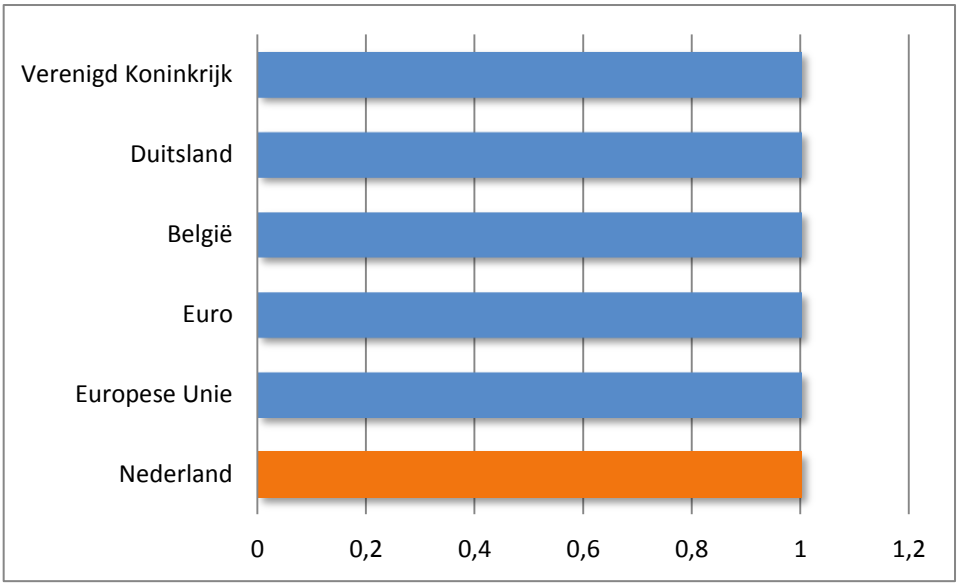
In 2010 zag 15% van de Nederlanders wel eens af van het aankopen van goederen of diensten via het internet, uit veiligheidsoverwegingen. Dit percentage is nagenoeg gelijk aan het gemiddelde percentage van de gehele Europese Unie.

In Nederland lijkt- in vergelijking met andere landen- veel vertrouwen te zijn in de veiligheid van online bankieren. Acht procent van de Nederlanders doet dit niet uit veiligheidsoverwegingen. Het Europees gemiddelde ligt op vijftien procent (zie grafiek 28).



Grafiek 28 – Geen online bankieren door zorgen Bron: Eurostat

Een van de factoren die het vertrouwen beïnvloed (sociale dimensie), is eerdere ervaring. Door een negatieve ervaring in het verleden, zijn gebruikers eerder geneigd om een soortgelijke dienst te mijden. Toch is het aantal gebruikers dat door eerder geleden financiële schade geen online transacties mee pleegt, zeer laag. Slechts een procent van de gebruikers heeft last gehad van financiële schade én besluit daardoor niet meer elektronisch te betalen (zie grafiek 29).



Grafiek 29 – Ooit financiële schade geleden daardoor geen online transacties Bron: Eurostat

Helaas ontbreken cijfers over het percentage mensen dat ooit financiële schade hebben geleden maar waarbij dit niet tot het stoppen van online transacties heeft geleid. Wel geeft Eurostat aan dat in 2009 1% van de Nederlanders problemen heeft gehad bij het kopen/verkopen via Internet die te relateren waren aan fraude. Door deze twee bronnen te combineren zou geconcludeerd kunnen worden dat 100% van de mensen die financiële schade hebben geleden, ook zijn gestopt met

het doen van online transacties, maar dit is zeker niet voldoende onderbouwd. Voor een toekomstig onderzoek is het interessant om dit verder uit te vragen.

5.3 Overzicht

In onderstaand overzicht zijn de onderzoeksresultaten samengevat die iets zeggen over het vertrouwen in ICT-diensten. Per resultaat wordt aangegeven op welke vertrouwensdimensie het resultaat betrekking heeft. Het eerste deel van de tabel bevat onderzoeksresultaten die op een algemeen niveau iets zeggen over vertrouwen in ICT-diensten. Het tweede deel van de tabel toont resultaten die meer specifiek betrekking hebben op de case study e-Commerce.

Algemeen	
Het percentage individuen dat in de afgelopen 12 maanden veiligheidsgerelateerde problemen heeft ondervonden bij internetgebruik voor persoonlijke doeleinden.	21%
Het percentage individuen dat zich zorgen maakt over het opdoen van virussen bij het gebruik van internet.	9%
Het percentage individuen dat uit veiligheidsoverwegingen af zag van het delen van persoonlijke informatie via sociale netwerken.	31%
Het percentage individuen dat uit veiligheidsoverwegingen af zag van contact met publieke diensten en administraties	5%
Het percentage individuen dat uit veiligheidsoverwegingen af zag van het downloaden van software, muziek, video's, games en overige data.	19%
Het percentage individuen dat uit veiligheidsoverwegingen af zag van het gebruik van mobiel internet via een verbinding van derden	9%
e-Commerce	
Het percentage individuen dat uit veiligheidsoverwegingen af zag van het bestellen of aankopen van goederen of diensten voor persoonlijk gebruik.	15%
Het percentage individuen dat uit veiligheidsoverwegingen af zag van online bankieren	8%
Het percentage individuen dat financiële schade leed via het internet en daardoor af ziet van online transacties	1%

5.3.1 Resultaten in relatie tot veiligheidsdimensies en actoren

De cijfers in de tabel geven een beeld van het percentage mensen dat problemen ondervond door - of zich zorgen maakten over - de veiligheid van de ICT-dienst en waarbij dit invloed had op de afweging de dienst wel of niet te gebruiken. Opvallend is hoe weinig data er beschikbaar is over het vertrouwen van gebruikers in ICT-diensten. Het ontbreken van andere onderzoeken, maakt het ook lastig om de cijfers in een perspectief te plaatsen. Ook is het niet altijd duidelijk waarom mensen zich zorgen maakten over de veiligheid van de dienst. Bijna een op de drie gebruikers ziet af van het delen van persoonlijke informatie over sociale netwerken uit veiligheidsoverwegingen. Dit kan komen door een gebrek aan institutioneel vertrouwen (bijvoorbeeld door het ontbreken van keurmerken of ontransparante *privacy policies*), maar kan ook worden beïnvloed door eerdere ervaringen uit de omgeving (sociaal), de inhoud van het product of de technologie.

Hoewel de resultaten een beeld geven in hoeverre veiligheidszorgen reden waren voor het uiteindelijk gebruik van een dienst, blijkt uit deze cijfers niet:

- Welke vertrouwensdimensies van invloed waren op de keuze voor het gebruik.
- Welke actoren dit vertrouwen hebben beïnvloed, of kunnen beïnvloeden in de toekomst.

Het gebrek aan inzicht in de twee bovenstaande punten, maakt het moeilijk om uitspraken te doen welke actoren een rol kunnen spelen in het vergroten van het vertrouwen. Uit deze cijfers blijkt niet of er een bottleneck zit bij de technologie, of bij de ervaringen uit de omgeving, of op een van de andere terreinen. Een gebruikersonderzoek zou de achterliggende motivaties meer helder kunnen maken.

Ook blijkt nog niet uit deze cijfers of de zorgen om veiligheidsproblemen terecht zijn. In de volgende paragraaf wordt meer specifiek gekeken naar de bronnen die iets zeggen over de feiten op dit terrein.

6 Conclusies en aanbevelingen

In dit onderzoek hebben we gekeken welke factoren het vertrouwen beïnvloeden. Daarbij hebben we expliciet gekeken naar de feitelijke veiligheid van ICT-diensten en de koppeling met de perceptie van de gebruiker.
In dit concluderende hoofdstuk zijn de belangrijkste resultaten nogmaals op een rij gezet en worden aanbevelingen gedaan voor de verdere ontwikkeling van de monitor.

6.1 Veiligheid ICT-diensten

Bij het onderzoek naar feiten is zoveel mogelijk gezocht naar statistieken die jaarlijks (of vaker) openbaar worden gemaakt. Dit maakt het mogelijk om ook het overzicht jaarlijks te actualiseren.

De belangrijkste bron hiervoor zijn de statistieken van Eurostat – een directoraat-generaal met als taak om de Europese Unie te voorzien van goede statistische informatie. In 2010 hebben zij een speciaal onderzoek gedaan naar informatiebeveiliging, wat veel relevante statistieken heeft opgeleverd. Het is te hopen dat ze dit onderzoek periodiek herhalen.

Een ander voorbeeld is het Intelligence Report van Microsoft, wat een gedetailleerd beeld geeft, maar is toegespitst op systemen met Microsoft software.

Wat opvalt bij de zoektocht naar cijfers is dat weinig informatie beschikbaar is over de infrastructuur:

- Beschikbaarheid/Uitval van Internet voor bedrijven
- Beschikbaarheid/Uitval van Internet voor consumenten
- Hoogte van financiële schade bij incidenten

Interpretatie feiten
Wanneer naar de resultaten wordt gekeken valt vooral op dat Nederland slechter scoort qua beveiligingsincidenten bij bedrijven:

	NL	UK	DE	BE	Euro
Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij informatie vernietigd of gecorrumpeerd is	**7%**	2%	2%	5%	6%
Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij ICT dienstverlening is verstoord door externe aanvallen	**7%**	2%	1%	3%	4%
Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij ICT dienstverlening is verstoord door hardware- of software-problemen	**19%**	4%	7%	12%	14%
Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij gevoelige informatie is uitgelekt door middel van IT aanvallen	**4%**	1%	0%	1%	1%
Het percentage Nederlandse bedrijven dat incidenten heeft gehad in 2010 waarbij (al dan niet opzettelijk) gevoelige informatie is uitgelekt door medewerkers	**4%**		1%	3%	1%

Wanneer wordt gekeken naar de uitrol van breedband internet naar bedrijven (zie ook Eurostat of de Marktrapportage Elektronische Communicatie) dan loopt Nederland wel voor op de bovengenoemde landen, maar dit verschil bedraagt maximaal 3% en verklaart dus niet het 200-300% hogere incident-ratio. Mogelijk wordt door Nederlandse bedrijven intensiever gebruik gemaakt van Internet. Een uitgebreider onderzoek zal moeten uitwijzen wat de belangrijkste oorzaken zijn.

Voor Spam (bij particulieren) geldt dat Nederlanders er meer last van hebben dan inwoners uit omringende landen – variërend van minimaal 11% (vergeleken met Duitsland) tot maximaal 26% (vergeleken met het Verenigd Koninkrijk). Als deze informatie wordt gecorreleerd aan het wekelijks gebruik van Internet door particulieren (waarbij Nederland respectievelijk 16% en 9% hoger scoort) dan is te zien dat een intensiever gebruik van Internet voor een groot deel verklaart waarom er meer particulieren zijn die last hebben van spam.

Tot slot scoort Nederland slecht op het vlak van particulieren die door internetgebruik te maken hebben gehad met misbruik van persoonlijke informatie (foto's, video's of persoonsgegevens die op community sites zijn geplaatst). 5% van de Nederlanders hebben hier last van gehad, terwijl het Verenigd Koninkrijk op 4% zit, en België en Duitsland op 2%. De reden hiervoor is onduidelijk en zou nader onderzocht moeten worden.

6.2 Vertrouwen in ICT-diensten

Er bleek weinig onderzoek beschikbaar over het vertrouwen in ICT-diensten. Wel bleek uit eenmalig onderzoek van Eurostat dat veiligheidsoverwegingen in sommige gevallen reden zijn om een dienst niet te gebruiken. Waarom deze veiligheidsoverweging in sommige gevallen de doorslag gaf en welke motivatie daaraan precies ten grondslag lag, bleek niet uit deze cijfers.

Wat opviel is dat Nederlanders, in verhouding tot andere Europese landen, zich weinig zorgen maken over virussen. Het percentage particulieren dat veel last heeft van spam en malware, ligt rond het gemiddelde.

Het is moeilijk gebleken op basis van bestaande cijfers uitspraken te doen over de impact van de (on)veiligheid van ICT-diensten op het vertrouwen van de gebruiker. Toch zijn er wel enkele verbanden die we willen benoemen.

Ook maken we ons weinig zorgen maken over de veiligheid van het internet bankieren. Toch zag 15% van de Nederlandse gebruikers af van het bestellen van goederen online uit veiligheidsoverwegingen. Dit zal naar verwachting niet komen door eerder geleden financiële schade, want het percentage gebruikers wat dat financiële schade ondervond én daardoor afzag van online winkelen, bedroeg slechts 1 procent.

Wat verder opvalt, is dat Nederlanders relatief vaak uit veiligheidsoverweging af zien van het delen van persoonlijke informatie via sociale netwerken. Waarom Nederlanders zich zorgen maken over de veiligheid van deze gegevens bij de betreffende dienst is niet duidelijk. Ook is het niet duidelijk in hoeverre deze gegevens gevaar lopen.

6.3 Vergroten van veiligheid en vertrouwen

6.3.1 Vergroten van veiligheid

Hoofdstuk vier toonde cijfers over de beschikbaarheid, integriteit, vertrouwelijkheid en gebruik van ICT diensten. Wat daar opvalt, is dat Nederland in de meeste gevallen rond het Europees gemiddelde scoort. Uitzondering is de hoeveelheid beveiligingsincidenten bij bedrijven, daarin scoort Nederland uitzonderlijk hoog.

Dat Nederland gemiddeld scoort als het gaat om deze veiligheidsindicatoren, wil niet zeggen dat er geen ruimte is voor verbetering. De oorzaken van de onveiligheden zijn moeilijk eenduidig te benoemen. Oplossingen zouden kunnen liggen in voorlichting of strengere regelgeving. Om hier meer uitspraken over te doen, zouden echter eerst de onderliggende oorzaken verder moeten worden onderzocht.

6.3.2 Vergroten van vertrouwen

In paragraaf 2.2 is omschreven dat veel ICT-diensten bestaan uit sub-elementen die door verschillende actoren vertegenwoordigd zijn (bijvoorbeeld de leverancier van technologie, third parties en de dienstaanbieder zelf). Voor de gebruiker is dit onderscheid niet altijd even transparant en het vertrouwen van de gebruiker zal daardoor vaak betrekking hebben op de dienst in zijn geheel. Het is in dit onderzoek niet duidelijk geworden in welke actoren het vertrouwen eventueel ontbreekt. Daardoor is ook moeilijk te zeggen welke actoren een rol hebben bij het vergroten van dat vertrouwen.

Eerder noemden we al dat vijftien procent van de gebruikers wel eens heeft afgezien van het aankopen van goederen of diensten online. Ook zien we dat er maar een kleine groep is die financiële schade leed door het gebruik van dergelijke diensten. De reden van wantrouwen ligt dus wellicht niet in de sociale dimensie (eerdere ervaring), maar mogelijk op een ander vlak zoals wantrouwen in de onderliggende technologie, de veiligheid van de transacties of de manier waarop de dienstverlener met de gegevens omgaat. Wanneer onvoldoende duidelijk is wat de precieze oorzaak is van het gebrek aan vertrouwen, is het ook niet goed mogelijk om de partij aan te wijzen die een rol heeft in het wegnemen van de onzekerheid bij

de gebruikers. Ook is niet te concluderen of het gebrek aan vertrouwen van de gebruiker, afslaat op de juiste actor. Het zou kunnen voorkomen dat de dienstleverancier door de gebruiker verantwoordelijk gehouden door een gepercipieerd veiligheidsrisico waar hij niet zelf verantwoordelijk voor is.

6.3.3 Aanbevelingen

De feitelijke veiligheid van ICT-diensten, voor zover gerapporteerd in dit onderzoek, scoort niet ver boven gemiddeld. Om verbeterpunten concreter te identificeren, is echter aanvullende informatie noodzakelijk.

In een vervolg onderzoek is het tevens zinvol om de oorzaken van een gebrek aan vertrouwen beter in kaart te brengen. Hierdoor kan ook beter worden bepaald:

- In hoeverre de veiligheidsperceptie van de gebruiker overeenkomt met het daadwerkelijke veiligheidsrisico.
- welke actor het vertrouwen kan verbeteren en zo de kans op gebruik van de dienst kan vergroten.

6.4 Monitoren van veiligheid en vertrouwen

In dit onderzoek is in kaart gebracht welke indicatoren kunnen worden gebruikt om het vertrouwen in ICT-diensten in kaart te brengen. De aanname die daarbij gedaan is, is dat vertrouwen een rol speelt bij de overweging om een dienst wel of niet te gebruiken. Daarnaast spelen andere factoren een rol, bijvoorbeeld het gebruiksgemak of de betaalbaarheid van de dienst, die in dit onderzoek buiten beschouwing zijn gelaten. Een andere gedane aanname is dat de perceptie van veiligheid van de dienst het vertrouwen beïnvloedt en dat deze perceptie deels wordt ingegeven door de feitelijke situatie.

Gebruik van ICT diensten stimuleert de economie, maar stimuleert ook participatie in de maatschappij op meerdere vlakken. Om een bijdrage te leveren aan deze ideale situatie, met in achtneming van bovenstaande aannames, is het bevorderlijk om én de veiligheidssituatie van ICT-diensten te optimaliseren en daarbij te bepalen welke factoren bijdragen aan een optimaal consumentenvertrouwen.

In dit project is een aanzet gemaakt tot een raamwerk dat veiligheid en vertrouwen over langere periode kan gaan monitoren. Het raamwerk bevat een uitgebreid palet van indicatoren die het speelveld goed af dekken. Het nadeel van deze breedte is dat er, zeker in dit eerste jaar, slechts delen van de indicatoren kunnen worden voorzien van data. Dit is mede te verklaren door de gekozen aanpak: deskresearch. Niet voor alle indicatoren is op dit moment data voorhanden. Ook de koppeling tussen de feitelijke veiligheid en het vertrouwen van gebruikers was daardoor moeilijk te maken.

Opvallend is dat veel cijfers op het gebied van vertrouwen iets zeggen over het uiteindelijk effect van (het ontbreken van) vertrouwen; bijvoorbeeld over het percentage van gebruikers dat uit veiligheidsoverwegingen afziet van gebruik van de dienst. Over de onderliggende motivatie, die meer inzicht geeft in de knelpunten en verbeterpunten- is nauwelijks informatie beschikbaar.
Aan de veiligheidskant speelt de gevoeligheid van de informatie ook een rol. Het is voor te stellen dat een bank weinig belang heeft om het aantal incidenten met daarbij behorende schade regelmatig naar buiten te communiceren als dit zijn

reputatie schaadt. Mede hierdoor zijn de cijfers op de niveaus van veiligheid en vertrouwen soms moeilijk aan elkaar te verbinden.

De aanpak om- naast de algemene cijfers- te werken met een specifieke casus, is goed bevallen. Omdat het speelveld zo groot is (veel diensten, actoren en technologieën), is enige afbakening noodzakelijk. Omdat vertrouwen vanuit een individu bekeken wordt, is een dienstafbakening logisch. Voor de veiligheidsfactoren komen dan automatisch de verschillende groepen indicatoren aan bod.

6.4.1 Aanbevelingen

Om het gekozen raamwerk beter te voorzien van data zou de deskresearch moeten worden uitgebreid met een gebruikersonderzoek om het vertrouwen en de onderliggende motieven beter in kaart te brengen. Dit gebruikers onderzoek zou meer inzicht kunnen geven in:

- De kennis van gebruikers over de feitelijke veiligheid
- De overwegingen om al dan niet gebruik te maken van een dienst (welke vertrouwens dimensies hebben de grootste invloed op het algehele vertrouwen)
- Het vertrouwen in verschillende actoren die betrokken zijn bij het aanbieden van de dienst (wordt een publieke dienst meer vertrouwd dan een commerciële dienst?)

Inzicht in deze vragen maakt het mogelijk om beter te identificeren welke partijen een rol hebben in het verbeteren van het vertrouwen. We bevelen aan om bij het opzetten van een gebruikersonderzoek te onderzoeken of aansluiting mogelijk is bij bestaande onderzoeken van bijvoorbeeld het CBS, Ernst & Young en de Europese surveys van Eurostat.

Om een beter beeld te krijgen van de veiligheidsincidenten zou, naast de deskresearch, ook interviews met branche- of consumentenorganisaties, of een survey, een aanvulling kunnen bieden om op een geaggregeerd niveau informatie te genereren.

7 Bronvermelding

7.1 Gebruikte informatie

Bron:
Eurostat 2010: Enterprises – ICT security policy, incidents and measures taken (isoc_ci_sce)
Eurostat 2010: Individuals – Internet security perceptions, incidences, precautions taken (isoc_ci_sci)
Eurostat 2010: e-Commerce by individuals and enterprises (isoc_ec)
Ernst & Young – ICT Barometer over cybercrime (25 maart 2011)
Microsoft – Security Intelligence Report (volume 10, 2010)
GData – Malware Report (2010)
Energiened.nl – Betrouwbaarheid E-netten in NL (2010)

Daarnaast is voor de informatie over het vertrouwen in ICT gebruik gemaakt van de volgende documenten:

Bron:
Xerox (Daniel W. Manchala) – E-Commerce Trust Metrics and Models (2000)
Ji-Hwan Lee, Soo Wook Kim, Chi Hoon Song – The effects of trust and perceived risk on users' acceptance of ICT services (2010)
Mary Ann Eastlick, Sherry L. Lotz, Patricia Warrington – Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment (2003)
Joshua Fogel, Elham Nehmad - Internet social network communities: risk taking trust and privacy concerns (2008)
Xueming Luo – Trust production and privacy concerns on the Internet (2000)
Tsai, Egelman, Cranor, Acquisti – The effect of online privacy information on purchasing behavior: an experimental study (2007)

7.2 Niet gebruikte informatie

Bron:	**Geen relevante informatie**	**Geen NL data**	**Niet over 2010**	**Duplicaat van gebruikte bron**
Ponemon – Cost of Data Breach (2010)		**X**		
Ponemon – Cost of Cyber Crime (2010)		**X**		
Cybersource – Online Fraud report		**X**		
Thuiswinkel.org – Online Betalen (2011)		**X**		**X**
Studiedienst van de Vlaamse Regering – ICT in Vlaanderen Internationaal vergeleken (2009)			**X**	**X**
TNO (T. Veugen, R. Coolen) – Measuring Information Security (2005)	**X**			
TNO (S. Huveneers, M. Geers) – Perceptieonderzoek Veilig Internet			**X**	
CERT – Research Annual Report (2009)	**X**	**X**	**X**	
Time.lex (voor EC) – Study on activities undertaken to address threats that undermine confidence in the Information Society, such as spam, spyware and malicious software (2008)	**X**		**X**	
Flash Eurobarometer (voor EC) – Data Protection in the European Union Citizens' perceptions (2008)			**X**	
Flash Eurobarometer (voor EC) – Information society as seen by EU citizens (2008)			**X**	**X**
Flash Eurobarometer (voor EC) – Confidence in the Information Society (2008)			**X**	
Govcert – Nationaal Trendrapport Cybercrime en Digitale Veiligheid (2010)	**X**			
Georgia Tech Information Security Center – Emerging Cyber Threats (2011)	**X**		**X**	
KLPD - Dienst Nationale Recherche - Overall-beeld Aandachtsgebieden (2010)	**X**			
McAfee – Threats Report (Q1 2010)	**X**			
Symantic – Messagelabs Intelligence (April 2010)	**X**		**X**	
OECD – The promotion of a culture of security for information systems and networks in OECD countries (2005)	**X**		**X**	
OECD - Scoping study for the measurement of trust in the online environment (2005)			**X**	**X**
OECD - APEC-OECD Workshop on security of information systems and networks – Summary (2005)	**X**	**X**	**X**	
OECD – Malicious Software (Malware): A Security Threat to the Internet Economy (2007)		**X**	**X**	
OECD - Measuring security and trust in the online environment: a view using official data (2008)			**X**	**X**
Van Eeten et. al. - The Role of Internet Service Providers in Botnet	**X**	**X**	**X**	

Bron:	**Geen relevante informatie**	**Geen NL data**	**Niet over 2010**	**Duplicaat van gebruikte bron**
Mitigation: An Empirical Analysis Based on Spam Data				