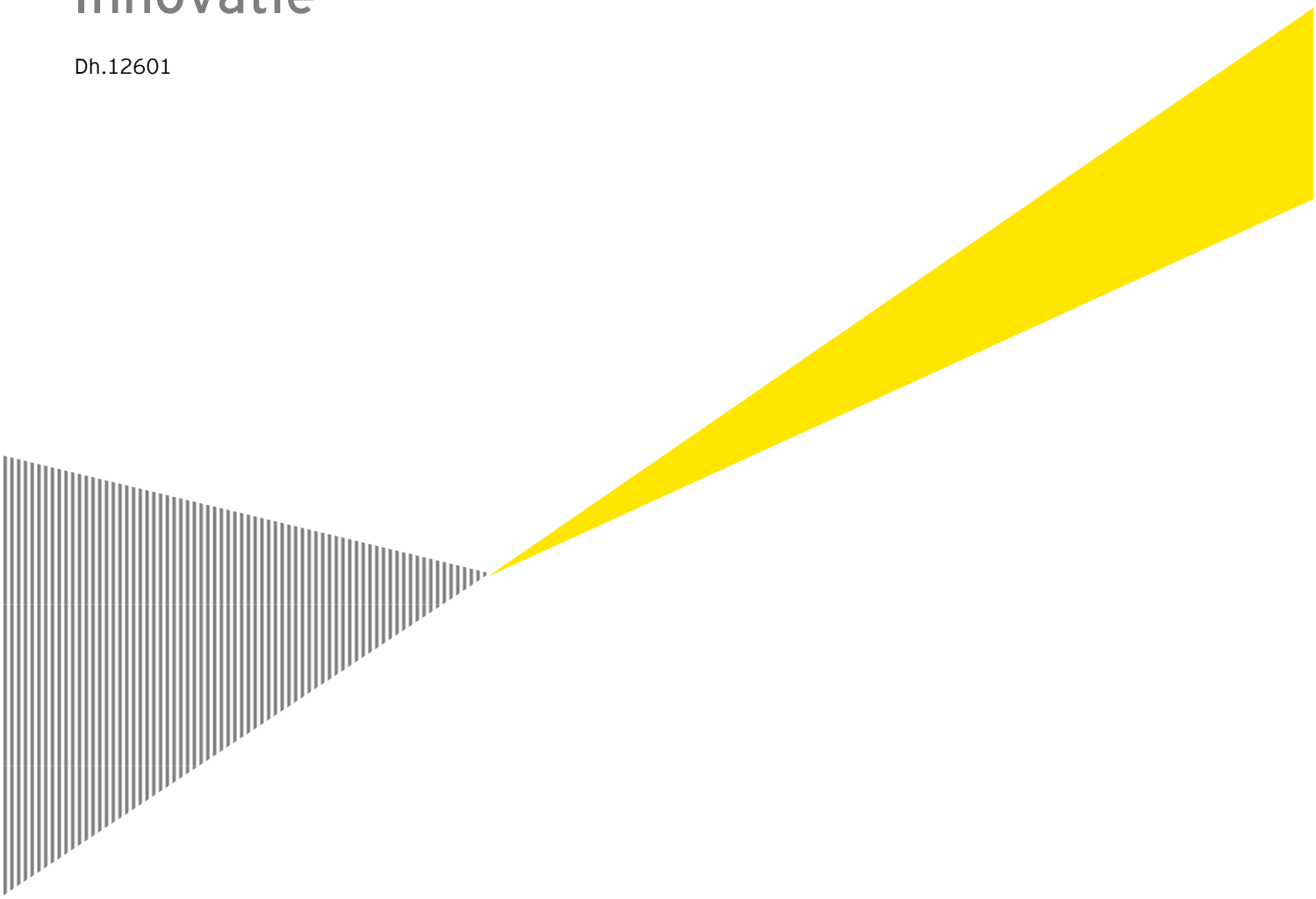
Ministerie van Economische Zaken, Landbouw & Innovatie

Dh.12601



Groeien door veiligheid

Onderzoek naar de waarde van een veilige en betrouwbare ICT infrastructuur voor de Nederlandse economie

ERNST & YOUNG

Inhoudsopgave

Managementsamenvatting

Inleiding

Dit onderzoek gaat over de economische meerwaarde van een veilige en betrouwbare ICT infrastructuur in Nederland. Daarbij definiëren wij de ICT infrastructuur als het geheel van de openbare datanetwerken en -verbindingen tussen organisaties en huishoudens (de basisinfrastructuur) en alle externe databases en informatiesystemen waarmee organisaties of huishoudens informatie uitwisselen. Interne bedrijfs- en thuisnetwerken vallen dus buiten de reikwijdte van het onderzoek.[1]

In het onderzoek stonden de volgende onderzoeksvragen centraal:

1 *In welke mate draagt een veilige en betrouwbare ICT-infrastructuur bij aan het Nederlandse vestigingsklimaat en aan duurzame economische groei in Nederland?*
2 *Hoe kan ons land zich op het terrein van ICT-veiligheid en -betrouwbaarheid onderscheiden van andere landen/EU lidstaten?*

Bij onderzoeksvraag 1 heeft daarbij de focus gelegen op drie belangrijke elementen die bepalend zijn voor de bijdrage van een betrouwbare en veilige ICT-infrastructuur aan de duurzame economische groeikansen van Nederland:

- de directe schade door veiligheids- en betrouwbaarheidsproblemen bij het bedrijfsleven in termen van productieverlies;
- de betekenis van een veilige en betrouwbare ICT-infrastructuur voor het Nederlandse vestigingsklimaat;
- de (meer)waarde van vertrouwen in de ICT aan de kant van de eindgebruiker (zakelijk en consumenten).

De waarde van minder directe schade bij het bedrijfsleven

Nederland beschikt over een hoogwaardig netwerk met een relatief hoge penetratie van breedbandverbindingen. Het Nederlandse bedrijfsleven maakt dan ook steeds meer gebruik van de mogelijkheden die het internet biedt voor bijvoorbeeld het ontvangen van orders, betalingsverkeer, faciliteren van thuiswerken, gegevensuitwisseling.

---

1 *De genoemde definitie vormt het uitgangspunt voor het onderzoek. Bij de interpretatie van de uitkomsten van het onderzoek dient er echter rekening mee gehouden te worden dat het begrip ICT infrastructuur niet duidelijk omlijnd is. Vaak is niet duidelijk waar ICT infrastructuur ophoudt en ICT toepassingen beginnen. Daarnaast kan een gebruiker van de infrastructuur niet altijd onderscheiden of problemen waarmee hij/zij geconfronteerd wordt te wijten zijn aan de externe ICT infrastructuur (bijv. een onveilige dataverbinding) of dat de problemen hun oorzaak vinden binnen het eigen interne netwerk.*

Een dergelijk hoogwaardig netwerk brengt ook kwetsbaarheden met zich mee. Voor Nederlandse bedrijven betekenen deze kwetsbaarheden dat zij geconfronteerd kunnen worden met ICT-gerelateerde veiligheids- en betrouwbaarheidsproblemen. In vergelijking met andere Europese landen worden Nederlandse bedrijven relatief veel getroffen door dergelijke problemen. Bijna de helft (2009: 43%) van de Nederlandse grote bedrijven wordt jaarlijks getroffen door ICT beveiligingsincidenten. Ter vergelijking: in Frankrijk en Duitsland is dit respectievelijk 20% en 22%.
Vermindering van het aantal incidenten kan het Nederlandse bedrijfsleven economische kansen bieden, onder andere doordat de schade die zij leiden als gevolg van die incidenten afneemt. In dit onderzoek hebben wij een globale inschatting gemaakt van de omvang van een deel van de directe schade die bedrijven ondervinden als gevolg van ICT-veiligheidsincidenten. Het onderzoek is daarbij geenszins volledig. Het verkrijgen van een volledig beeld vereist een veel omvangrijker onderzoek[2].

Uit onderzoek van Ernst & Young naar cybercrime komt naar voren dat één op de drie bedrijven in Nederland in 2010 schade heeft ondervonden als gevolg van cybercrime. Een op de vijf bedrijven leed hierdoor ook directe financiële schade. De omvang van deze financiële schade varieert per bedrijf (van minder dan 10.000 euro tot meer dan 1 miljoen euro). De omvang van deze directe financiële schade voor de Nederlandse economie is aanzienlijk.

In het onderzoek heeft de nadruk gelegen op de volgende twee directe schadeposten voor het bedrijfsleven:

- het productieverlies als gevolg van netwerkuitval;
- het productieverlies als gevolg van ontvangen en verwerken van spam.

In Tabel S.1 zijn de resultaten van de analyse van deze schade posten weergegeven. Het beperken van de tijd die werknemers bezig zijn met het lezen en verwerken van spam belangrijke economische kansen biedt. Wij schatten deze schadepost voor 2010 in op 1 tot 2 miljard euro. Dat is 150 tot 300 euro per werknemer per jaar. Vooral binnen kleinere bedrijven zijn werknemers per dag relatief veel tijd kwijt met de verwerking van spam. Met name hier liggen dan ook kansen voor verbetering.

2 *Andere belangrijke schadeposten zoals de schade door digitale diefstal van vertrouwelijke informatie (klantgegevens, inlogcodes, bedrijfsgegevens), het omzetverlies bij bedrijven als gevolg van het tijdelijk niet beschikbaar zijn van de website en de schade als gevolg van diefstal van vertrouwelijke informatie zijn niet verder uitgewerkt in het onderzoek. Er is niet voldoende informatie bekend om (binnen dit onderzoek) tot een goede inschatting te komen van de omvang van deze schadeposten. Ook cascade-effecten zijn buiten beschouwing gelaten.*

Tabel S.1 Overzicht globale inschatting productieverlies in Nederland als gevolg van netwerkuitval en spam – 2010.

	Door oorzaken van buiten de eigen organisatie	Door oorzaken binnen de eigen organisatie
Productieverlies door netwerkuitval	100-150 mln. euro	200-300 mln. euro
Productieverlies als gevolg van spam	1 – 2 mld. euro	N.v.t.
Totaal productieverlies als gevolg van netwerkuitval en spam	**1,1 – 2,2 mld. euro**	**0,2 – 0,3 mld. Euro**

Naast de schade die het bedrijfsleven ondervindt als gevolg van ICT betrouwbaarheids- en veiligheidsproblemen doet zij ook investeringen om dergelijke problemen te voorkomen. Uit ons onderzoek komt naar voren dat bedrijven en non-profitorganisaties in 2010 gemiddeld 17 procent van hun totale ICT-budget hebben besteed aan ICT veiligheid[3].

Betekenis voor het vestigingsklimaat

Nederland beschikt over een kwalitatief hoogwaardige ICT-infrastructuur. Op vestigingsplaatslijstjes staat Nederland op het terrein van de aantrekkelijkheid van ICT en Telecom in de Europese top 5. Dat is belangrijk, want de kwaliteit van de telecom infrastructuur wordt in internationale onderzoeken genoemd als een van de drie meest bepalende vestigingsplaatsfactoren.

Nederlandse managers en ICT-professionals waarderen de *veiligheid en betrouwbaarheid* van de Nederlandse ICT-infrastructuur als beter dan die van India, China, Frankrijk en België. Denemarken en Duitsland worden juist hoger gewaardeerd.

Op basis van ons onderzoek concluderen wij dat de *veiligheid en betrouwbaarheid* van de ICT-infrastructuur voor bedrijven die overwegen zich te vestigen in Nederland geen doorslaggevende factor bij deze beslissing. Veiligheid en betrouwbaarheid van de ICT-infrastructuur lijkt vooral op de achtergrond een rol speelt. Andere factoren, zoals politieke stabiliteit, de beschikbaarheid van geschoold personeel en het rechtsbestel, maar ook de snelheid van ICT verbindingen spelen een grotere rol. Er is een minimaal noodzakelijk niveau van veiligheid en betrouwbaarheid van de ICT-infrastructuur nodig. Ligt het niveau onder dit minimum niveau dan geldt het als een negatieve vestigingsplaatsfactor, maar ligt het niveau boven het minimum dan lijkt een nog hoger niveau voor vestigingsplaatsbeslissingen (op enkele specifieke typen bedrijvigheid na) geen grote rol meer te spelen en zijn andere factoren belangrijker. Nederland voldoet volgens de respondenten in ons onderzoek op dit moment ruimschoots aan dit niveau. Tegelijkertijd blijkt uit cijfers van Eurostat dat relatief veel Nederlandse bedrijven in 2009 getroffen werden door ICT veiligheidsincidenten. Dat het op dit moment niet speelt, betekent dus niet dat er geen blijvende aandacht nodig is.

3 *Daarnaast doen ook consumenten, de netwerkserviceproviders en de overheid investeringen om de ICT veiligheid te verhogen. Deze zijn in dit onderzoek niet in beeld gebracht.*

Meerwaarde van vertrouwen bij de eindgebruiker

Het vertrouwen van consumenten en bedrijven in de veiligheid en betrouwbaarheid van de Nederlandse ICT-infrastructuur is een bepalende factor voor het gebruik dat zij maken van die infrastructuur. Bij vertrouwen gaat het daarbij om verschillende aspecten, zoals het vertrouwen dat er geen misbruik wordt gemaakt van persoonlijke gegevens en dat de privacy niet geschonden wordt, vertrouwen dat financiële transacties op een veilige manier plaatsvinden en vertrouwen dat goederen en diensten die online worden besteld ook geleverd worden. Ook het vertrouwen in de beschikbaarheid is van belang.

Vertrouwen bij het bedrijfsleven
Uit ons onderzoek blijkt dat Nederlandse bedrijven vertrouwen hebben in de ICT-veiligheid van hun eigen organisatie. Tegelijkertijd legt vier op de tien bedrijven zich als gevolg van veiligheidsissues beperkingen op in het gebruik van de technische mogelijkheden op het terrein van ICT. Daardoor maken bedrijven niet of niet volledig gebruik maken van de (technische) mogelijkheden om de dienstverlening aan de klant te digitaliseren of om informatiestromen te digitaliseren. Het gebruik van dergelijke technische mogelijkheden biedt kansen voor bedrijven om productiviteitsvoordelen te behalen.

Uit het onderzoek komen twee belangrijke uitdagingen met betrekking tot het vertrouwen bij het bedrijfsleven naar voren:

1 Versterken van het vertrouwen van bedrijven in de ICT infrastructuur. Uit ons onderzoek komt naar voren dat managers en professionals binnen Nederlandse bedrijven de veiligheid van de Nederlandse ICT infrastructuur beoordelen met het rapportcijfer 6,7 en de betrouwbaarheid een 6.9. Dit rapportcijfer laat zien dat, hoewel de grondhouding positief is, er volgens de bedrijven nog zeker ruimte is voor verbetering. Die ligt bijvoorbeeld in de verbetering van de controleerbaarheid van de datastromen. Dit kwaliteitsaspect krijgt het laagste rapportcijfer: een 6,3.
2 Meer inzicht in kosten en voordelen van verdere investeringen: Het grote vertrouwen van bedrijven in de eigen ICT beveiliging heeft als risico dat het een belemmering kan vormen voor het verder benutten van de kansen op verdere productiviteitsverbetering. Een belangrijke uitdaging ligt daarbij in een realistische beeldvorming van het beveiligingsniveau van de eigen organisatie van bedrijven en van de voordelen van het investeren in de kansen die ICT nog biedt.

Vertrouwen bij consumenten
Op basis van een doorvertaling van een Europese analyse van Booz & Co naar het Nederlandse niveau, schatten wij in dat in Nederland een versterking van het vertrouwen in het internet bij de Nederlandse consument in 2014 potentieel tot (bruto) 1,2 miljard meer omzet aan verkopen van producten en diensten via internet kan leiden. Deze extra groei in internetverkopen kan worden gerealiseerd door het bestede bedrag van consumenten die ook op dit moment al online aankopen doen te verhogen of door de bezwaren weg te nemen bij de groep consumenten die dit op dit moment nog niet doet, omdat zij bezorgd is over de veiligheid van online betalingstransacties. Bij beide groepen ligt potentie.

De groep Nederlandse consumenten die al wel online producten of diensten koopt, besteedt jaarlijks ruim 800 euro online. In vergelijking met andere Europese landen is dat relatief laag.

Waar de Nederlandse consument in 2009 ruim 800 euro online uitgaf, gaven de Deense en Britse consumenten meer dan 1.200 euro uit. In 2009 maakte de online omzet uit de verkoop van producten en diensten via het internet (e-commerce) ongeveer 1% uit van de totale Nederlandse economie. Daarmee blijft Nederland achter op een aantal andere EU-landen, zoals het Verenigd Koninkrijk en Denemarken waar e-commerce rond de 2% van de economie uitmaakt (zie Tabel S.2).

Tabel S.2: Benchmark Europese landen op het terrein van "online verkoop" (2009)

	Percentage online consumenten	Online verkoop per consument (in €)	Online verkoop (in mld. €)	Online verkoop als % BNP
Verenigd Koninkrijk	66%	1239,51	42,7	1,98%
Denemarken	64%	1213,25	3,9	1,92%
Finland	54%	975,56	2,6	1,41%
Noorwegen	-	1101,69	3,3	1,30%
Frankrijk	45%	994,65	24,7	1,19%
Duitsland	56%	764,98	33,4	1,19%
Nederland	***63%***	***857,00***	***7,4***	***1,16%***
Zweden	63%	801,79	3,8	1,13%
Spanje	23%	778,65	6,3	0,47%
Italië	12%	934,67	8,2	0,45%

Bron: Eurostat, Kelkoo, CIA World Factbook, Thuiswinkel.org

Hoewel de oorzaak van het verschil in het bestede bedrag per consument niet direct gelegen is in vertrouwensaspecten, biedt het versterkt inzetten op meer vertrouwen in de veiligheid van internet bij consumenten wel mogelijkheden om deze achterstand in te lopen.

Naast de groep die al wel online koopt is er een omvangrijke groep van ongeveer één miljoen consumenten die op dit moment geen producten online aanschaft, (onder andere) omdat zij geen vertrouwen hebben in de veiligheid van online betalingstransacties, in de privacy van de verstrekte gegevens of in de betrouwbaarheid van de levering. Zouden al deze consumenten dit wel doen en ook hetzelfde bedrag besteden als de gemiddelde online consument dan levert dat 900 miljoen euro aan extra online omzet op. Of deze potentie wordt benut hangt onder andere af van andere bezwaren die deze consumenten eventueel hebben bij het kopen op internet.

Consumenten maken zich relatief veel zorgen over misbruik van persoonlijke gegevens, schending van privacy en financiële schade door phishing of fraude met betaalmiddelen, terwijl maar een zeer klein deel van de consumenten daar zelf door getroffen wordt. Een belangrijke uitdaging ligt er dan ook in om consumenten meer vertrouwen te geven dat er goed met hun gegevens wordt omgegaan en dat betalen via internet veilig is.

Tegenover de economische potentie van een hoger vertrouwen staat een potentieel economisch risico wanneer het vertrouwen afneemt. In de interviews wordt er op gewezen dat dit risico qua omvang in potentie groter is dan de huidige directe schade die bedrijven op dit moment ondervinden als gevolg van ICT veiligheidsproblemen.

Booz & Co schat in haar analyse in dat dit risico in economische termen een omvang heeft van ongeveer tweemaal de extra economische potentie bij een toename van het vertrouwen.

Aanbevelingen

In dit rapport staan de economische kansen van een veilige en betrouwbare ICT infrastructuur centraal. Of deze economische kansen ook gerealiseerd worden hangt enerzijds af van de mate waarin de veiligheid en betrouwbaarheid (ondanks de toenemende complexiteit) kan worden behouden en verstevigd. Anderzijds is het vertrouwen van consumenten en bedrijven van groot belang om de kansen te benutten.

Maatregelen van de overheid en de marktpartijen zijn ook op dit moment al gericht op het versterken van de veiligheid en betrouwbaarheid en het vertrouwen bij de eindgebruiker. Wij bevelen aan deze maatregelen te handhaven en verder te versterken[4].
Naast het behoud en het versterken van maatregelen die ook nu reeds worden genomen doen wij de volgende aanbevelingen:

1 **Investeer in het terugdringen van spam voor het MKB.** Uit ons onderzoek komt naar voren dat de dagelijkse last op jaarbasis een behoorlijke kostenpost oplevert, met name voor het MKB. Voorlichting richting het MKB over de kosten en baten van een goede spambestrijding kan per saldo voor bedrijven veel efficiencywinst opleveren.

2 **Maak bedrijven meer bewust van de eigen verantwoordelijkheid, maar biedt ook hulp om die op te pakken:** Uit ons onderzoek komt het beeld naar voren dat de veiligheid en betrouwbaarheid van de Nederlandse ICT infrastructuur versterkt kan worden door bedrijven bewuster te maken van hun verantwoordelijkheid in deze, zowel op het terrein van de veiligheid als de betrouwbaarheid. Tegelijkertijd worden de risico's en de te nemen maatregelen om die risico's te beperken steeds complexer. Voor (kleinere) bedrijven is dit steeds moeilijker te overzien. Er is daarom in toenemende mate ook een rol weggelegd voor bijvoorbeeld service providers, financiële dienstverleners, de aanbieders van online diensten om bedrijven daarin te ondersteunen door het (gratis of tegen vergoeding) bieden van oplossingen of voorlichting.

3 **Geef het bedrijfsleven inzicht in kosten en baten van nog bestaande productiviteitsverbeteringen:** Uit het onderzoek komt naar voren dat bedrijven ondanks een hoog vertrouwen in de eigen ICT beveiliging toch mogelijkheden tot productiviteitsverbetering onbenut laten vanwege veiligheidsredenen. Mogelijk denken bedrijven dat er geen technische mogelijkheden zijn om de veiligheidsbelemmeringen die zij zien weg te nemen of hebben zij het beeld dat hier omvangrijke investeringen voor nodig zijn die niet opwegen tegen de voordelen van deze investeringen in termen van toegenomen productiviteit of toename van de omzet. Voorlichting over mogelijkheden hiertoe, de kosten hiervan, maar ook baten kan bedrijven het vertrouwen geven om verder te investeren in ICT mogelijkheden.

---

4 *Daarbij gaat het uiteraard wel steeds om een afweging tussen veiligheid en innovativiteit. Te stringent beleid en regelgeving rond ICT veiligheid kan innovatie en bedrijvigheid ook belemmeren, doordat bijvoorbeeld diensten daardoor niet geleverd kunnen worden of doordat daardoor consumenten zich in hun privacy aangetast voelen.*

4 **Versterk de controleerbaarheid van datastromen over de infrastructuur voor bedrijven:** Bedrijven beoordelen de controleerbaarheid van de ICT infrastructuur als matig (een rapportcijfer 6,3). Het gaat daarbij om de mate waarin te controleren is of gegevens juist, volledig en tijdig zijn uitgewisseld. En: de mate waarin de oorzaak te achterhalen is wanneer dit niet het geval is. Het vertrouwen van Nederlandse bedrijven in de Nederlandse ICT infrastructuur kan versterkt worden door de controleerbaarheid van datastromen te versterken.
Wij bevelen dan ook aan samen met de service providers te onderzoeken hoe de controleerbaarheid voor bedrijven verbeterd kan worden.

5 **Verhoog het vertrouwen van consumenten in de veiligheid en privacy van persoonsgegevens op internet:** Voor ongeveer een kwart van de consumenten die nog geen online aankopen doen, spelen privacyaspecten hierbij een belangrijke rol. Door consumenten meer zekerheid te bieden dat de veiligheid en de privacy van de gegevens die zij achter laten gegarandeerd is, kan het vertrouwen van consumenten in internet verder worden versterkt. Dat kan bijvoorbeeld door in de bestaande keurmerken het privacybeleid te versterken of meer naar voren te brengen in de communicatie.

6 **Zorg voor meer helderheid over de betrouwbaarheid van internetbedrijven:** Meer helderheid in de betrouwbaarheid van internetwinkels kan het vertrouwen van consumenten verder versterken. Diverse keurmerken hebben tot doel om deze betrouwbaarheid te garanderen. Mogelijkheden liggen bijvoorbeeld in het versterken van deze keurmerken (uitbreiden criteria voor deelname), of harmonisatie (samenvoegen keurmerken). Samen met de aanbieders van de keurmerken kan onderzocht worden hoe de overheid hier een bijdrage aan kan leveren.

7 **Onderzoek mogelijkheden wegnemen risico's bij de consument:** Ter versterking van het vertrouwen in de ICT infrastructuur bij consumenten kunnen naast communicatie ook andere middelen worden ingezet. Een alternatieve maatregel zou bijvoorbeeld kunnen liggen in het verschuiven van het risico op schade van de consument naar de internetdienstverlener. Dat kan bijvoorbeeld door consumenten een financiële compensatie te geven wanneer zij buiten hun schuld om worden geconfronteerd met veiligheidsproblemen, financiële schade, of netwerkuitval. Een andere mogelijkheid is de ontwikkeling van een garantiefonds voor internetwinkels, die consumenten de garantie van levering biedt, ook wanneer de oorspronkelijke aanbieder niet in staat is om te leveren of weigert aan de aangegane verplichting te voldoen. Nader onderzoek kan uitwijzen of een dergelijke aanpak effectief is.

8 **Werken aan vertrouwen en veiligheid vereist samenwerking en een heldere regie:** Bij het op peil houden en versterken van de betrouwbaarheid en veiligheid van de Nederlandse ICT infrastructuur en het vertrouwen bij de eindgebruiker hierin zijn vele partijen betrokken (netwerkaanbieders, overheid, financiële dienstverleners, aanbieders van diensten). Hoewel er tussen deze partijen al we samengewerkt wordt, willen wij het belang van een verdere versterking van de samenwerking hier onder de aandacht brengen. Alleen vanuit een gezamenlijke visie en afstemming van activiteiten gericht op de verbetering van ICT veiligheid over de partijen heen kan de economische potentie van een groter vertrouwen bij bedrijven en consumenten in de ICT veiligheid volledig worden gerealiseerd. Ook een meer eenduidige regie vanuit de overheid kan daaraan bijdragen.

9 **Aanbevelingen voor verder onderzoek.** Bij de start van het onderzoek was reeds duidelijk dat deze studie geen volledig antwoord zou kunnen geven op de vraag wat de economische meerwaarde is van een veilige en betrouwbare ICT infrastructuur. De problematiek rond ICT veiligheid en de doorwerking daarvan in de economie is dusdanig complex dat hiervoor een uitgebreider onderzoek noodzakelijk is. Uit ons onderzoek komen de volgende aangrijpingspunten voor vervolgonderzoek naar voren:

— *Verdiepend onderzoek naar de schade van ICT veiligheids- en betrouwbaarheidsproblemen.* We bevelen aan een dergelijk onderzoek in nauwe samenwerking met alle relevante partijen op de Nederlandse ICT markt uit te voeren. Het commitment van deze partijen is van groot belang aangezien belangrijke delen van de benodigde informatie alleen voorhanden is bij deze partijen.

— *Nader onderzoek naar de economische meerwaarde van vertrouwen* in de veiligheid en betrouwbaarheid van de ICT-infrastructuur bij de eindgebruiker verdiepende inzichten geven. Wij denken dan bijvoorbeeld aan onderzoek naar de relatie tussen het gebruik van internet door consumenten en vertrouwen in ICT veiligheid en betrouwbaarheid en aan een verdere verdieping van de inschatting van de totale economische potentie en het economische risico van vertrouwen.

1 Inleiding

1.1 Aanleiding voor het onderzoek

De afhankelijkheid van ICT is de afgelopen jaren enorm gegroeid en blijft ook in de toekomst verder toenemen. Het aandeel van de verkoop van producten en diensten via het internet neemt een steeds prominentere rol in. Steeds meer burgers, overheden en bedrijven maken gebruik van openbare datanetwerken voor het uitwisselen van gegevens, het koppelingen van informatiesystemen en basisregisters (bijvoorbeeld Gemeentelijke Basis Administratie, GBA), het aansturen van vitale infrastructuren (energiecentrales, beveiligingssystemen, kustbewaking, matrixinformatie, verkeersregeling, etc.) en het opslaan van persoonlijke gegevens (bijvoorbeeld het Elektronisch Patiënten Dossier, EPD). Er is steeds verdere toegang tot persoonlijke gegevens via webpagina's en online sociale netwerken, zoals Twitter, LinkedIn en Facebook. ICT zorgt ervoor dat processen efficiënter verlopen, bureaucratie vermindert en klanten steeds persoonlijker benaderd kunnen worden.

Naast deze voordelen brengt de stijgende afhankelijkheid van ICT ook veiligheidsrisico's met zich mee. Veilige/betrouwbare ICT wordt steeds belangrijker. Praktisch alle informatie van belang voor ondernemer en burger wordt immers vastgelegd in informatiesystemen. De veiligheid en betrouwbaarheid van ICT is cruciaal omdat kritieke informatie integer, beschikbaar en exclusief moet zijn zodat deze vertrouwelijk behandeld kan worden. Bij de verwerking en opslag van gegevens dient rekening te worden gehouden met de Wet Bescherming Persoonsgegevens (privacy) en het vertrouwelijk houden van concurrentiegevoelige bedrijfsinformatie. Ook dient rekening gehouden te worden met cyber criminaliteit. Financiële instellingen zijn bijvoorbeeld een gewild doelwit. Internetcriminelen kunnen via namaak webapplicaties login gegevens van bankklanten achterhalen en zodoende op digitale wijze geld stelen. Dit leidt tot directe financiële schade bij bedrijven en particulieren, en indirecte financiële schade voor financiële instellingen door imagoaantasting en afname van vertrouwen.

Het ministerie van Economische Zaken, Landbouw & Innovatie (EL&I) heeft de beleidsverantwoordelijkheid voor de telecomsector en een coördinerende taak met betrekking tot ICT. Het ministerie van EL&I is daarom belast met vraagstukken die de veiligheid en betrouwbaarheid van de ICT-infrastructuur en haar toepassingen raken. Tegen de achtergrond van ontwikkelingen in de markt en maatschappij zoekt EL&I in het ICT-veiligheidsbeleid de balans tussen consumenten-, bedrijfs- en publieke belangen. Investeren in een veilige en betrouwbare ICT-infrastructuur heeft een positieve invloed op de economische groei, maar brengt ook kosten met zich mee. Het is daarom van belang om de afweging te maken of de kosten die gemoeid zijn met een verdere verhoging van de veiligheid/betrouwbaarheid van de ICT-infrastructuur opwegen tegen de maatschappelijke baten die deze investeringen opleveren. Vanuit economisch perspectief is daarbij een belangrijke vraag welke bijdrage een veilige en betrouwbare ICT-infrastructuur levert aan het Nederlandse vestigingsklimaat en aan de economische groeikansen van ons land.

1.2 Onderzoeksvragen

Doel van het onderzoek was meer inzicht te krijgen in de bijdrage van een betrouwbare en veilige ICT-infrastructuur voor de duurzame economische groeikansen van Nederland.

In het onderzoek stonden hierbij de volgende onderzoeksvragen centraal:

1 *In welke mate draagt een veilige en betrouwbare ICT-infrastructuur bij aan het Nederlandse vestigingsklimaat en aan duurzame economische groei in Nederland?*
   a. *Wat is de (potentiële) relatieve bijdrage van (veilige/betrouwbare) ICT aan de economische groeikansen van Nederland?*
   b. *Wat is de relatieve betekenis van (veilige/betrouwbare) ICT bij de vestigingsplaatskeuze van bedrijven en hoe scoort Nederland ten opzichte een aantal relevante andere landen het terrein van veilige ICT als vestigingsplaatsfactor?*
   c. *Wat is de (meer)waarde van vertrouwen in de ICT-sector en specifiek in relatie tot veilige netwerken en informatiebeveiliging aan de kant van de eindgebruiker?*

Gezien de beperkte doorlooptijd en de brede vraag die aan het onderzoek ten grondslag lag, is er bij de start veel aandacht besteed aan de afbakening van het onderzoek. In hoofdstuk 2 gaan we hier nader op in. In overleg met de opdrachtgever is besloten het onderzoek te focussen op drie belangrijke elementen die bepalend zijn voor de bijdrage van een betrouwbare en veilige ICT-infrastructuur aan de duurzame economische groeikansen van Nederland:

- de directe schade door veiligheids- en betrouwbaarheidsproblemen bij het bedrijfsleven in termen van productieverlies;
- de betekenis van een veilige en betrouwbare ICT-infrastructuur voor het Nederlandse vestigingsklimaat;
- de (meer) waarde van vertrouwen in de ICT aan de kant van de eindgebruiker (zakelijk en consumenten).

2 *Hoe kan ons land zich op het terrein van ICT-veiligheid en -betrouwbaarheid onderscheiden van andere landen/EU lidstaten?*
   a. *Waarin kan Nederland zich onderscheiden en waarin moet Nederland juist samen optrekken met andere (EU-lid)staten met betrekking tot een veilige/betrouwbare IC- infrastructuur in relatie tot economische groeimogelijkheden en vestigingsklimaat?*
   b. *Specifiek op ICT-veiligheidsterrein: Is veiligheid van netwerken/ informatiebronnen en vertrouwen vooral afhankelijk van grote incidenten of meer van dagelijkse vervelende hinder?*

1.3 Onderzoeksaanpak

Het onderzoek is uitgevoerd in de volgende fasen:

Fase 1: Voorbereiding

Het onderzoek is van start gegaan met een fase waarin de scope en het analysekader van het onderzoek is vastgesteld. In hoofdstuk 2 is de uitwerking hiervan weergegeven.

Fase 2: Dataverzameling

Om te komen tot een goede onderbouwing van het eindresultaat hebben wij gebruik gemaakt van de volgende drie onderzoeksmethoden:

- **Onderzoek van bestaande bronnen.** Analyse van onderzoeksrapporten, wetenschappelijke studies, statistieken en databestanden, waaronder de resultaten van eerdere relevante onderzoeken van Ernst & Young zoals de ICT-barometer, de Global Information Security Survey en de European Attractiveness Survey. Daarnaast zijn ook andere bronnen onderzocht, zoals onderzoeken van het CBS, het SCP en Eurostat.

- **Webenquête.** Wij hebben hierbij gebruik gemaakt van het online panel dat Ernst & Young regelmatig bevraagt in het kader van de ICT-barometer. Het betreft een panel van directeuren, managers en professionals uit het bedrijfsleven en de (semi)overheid.

  In de webenquête hebben wij vragen gesteld op het gebied van:
  - een beoordeling van de huidige betrouwbaarheid/veiligheid van de ICT-infrastructuur in Nederland;
  - het productieverlies van bedrijven als gevolg van een onveilige/onbetrouwbare ICT-infrastructuur;
  - de mate waarin een betrouwbare en veilige ICT-infrastructuur voor hun bedrijf een belangrijke vestigingsplaatsfactor is (in vergelijking met andere vestigingsplaatsfactoren).

  In totaal hebben 602 respondenten de vragen beantwoord.

  De resultaten van de ICT Barometer zijn representatief voor de groep van directeuren, managers en professionals in Nederland. Deze groep werkt relatief vaak bij grote bedrijven in de dienstverlenende sector. Kleine bedrijven (<20 werknemers) en bedrijven in de productie/industrie zijn in de respons ondervertegenwoordigd.

- **Face-to-face interviews.** Met brancheorganisaties en bedrijven uit de ICT-sector, het bank- en verzekeringswezen, handelsmaatschappijen en de transportsector. Doel van de gesprekken was enerzijds om inzicht te krijgen in de mening op brancheniveau over het belang van een veilige en betrouwbare ICT-infrastructuur voor de economische groeikansen van Nederland en het Nederlandse vestigingsklimaat. Anderzijds zijn de diepte interviews gebruikt om nader inzicht te krijgen in de richtingen waarin Nederland zich kan onderscheiden op het terrein van een veilige/betrouwbare ICT-infrastructuur.

  In bijlage I is een overzicht weergegeven van de geïnterviewde organisaties.

Fase 3: Analyse en rapportage

Het onderzoek is afgesloten met een fase waarin de uitkomsten van het onderzoek zijn geanalyseerd en verwerkt tot deze rapportage. Ter verificatie van de resultaten zijn deze binnen Ernst &Young voorgelegd aan een groep materiedeskundigen op het terrein van ICT-veiligheid en economische ontwikkeling en investeringsklimaat.

1.4 Leeswijzer

Het rapport kent de volgende opbouw:

- In hoofdstuk 2 wordt ingegaan op de afbakening van het onderzoek. Daarbij wordt ingegaan op de afbakening van het begrip ICT infrastructuur en de begrippen veiligheid en betrouwbaarheid. Ook wordt de vraagstelling afgebakend.
- In hoofdstuk 3 wordt een analyse gegeven van de problemen die Nederlandse bedrijven ondervinden met de Nederlandse ICT infrastructuur. Voor een deel van de problemen werken we vervolgens een schatting uit van de economische schade die hierdoor wordt geleden.
- Hoofdstuk 4 gaat over het vertrouwen in de ICT infrastructuur bij de eindgebruiker (bedrijven en consumenten) en de economische potentie van een hoger vertrouwen.
- In hoofdstuk 5 staat het belang van een veilige en betrouwbare ICT infrastructuur voor het Nederlandse vestigingsklimaat centraal.
- In hoofdstuk 6 werken we de belangrijkste conclusie van het onderzoek uit en geven we een aantal aanbevelingen op basis van het uitgevoerde onderzoek.
- In de bijlagen zijn opgenomen: een overzicht van de geïnterviewde bedrijven en brancheorganisaties (bijlage I) en een nadere uitwerking van het begrip veiligheid en betrouwbaarheid (bijlage II).

2 Afbakening onderzoek

2.1 Inleiding

Ernst & Young heeft onderstaand analysekader gebruikt in het onderzoek naar de bijdrage van veilige en betrouwbare ICT-infrastructuur aan de economische groeikansen in Nederland.

Figuur 2.1 Analysekader.

In de onderstaande paragrafen werken we dit analysekader nader uit.

2.2 Het economisch belang van een veilige en betrouwbare ICT-infrastructuur

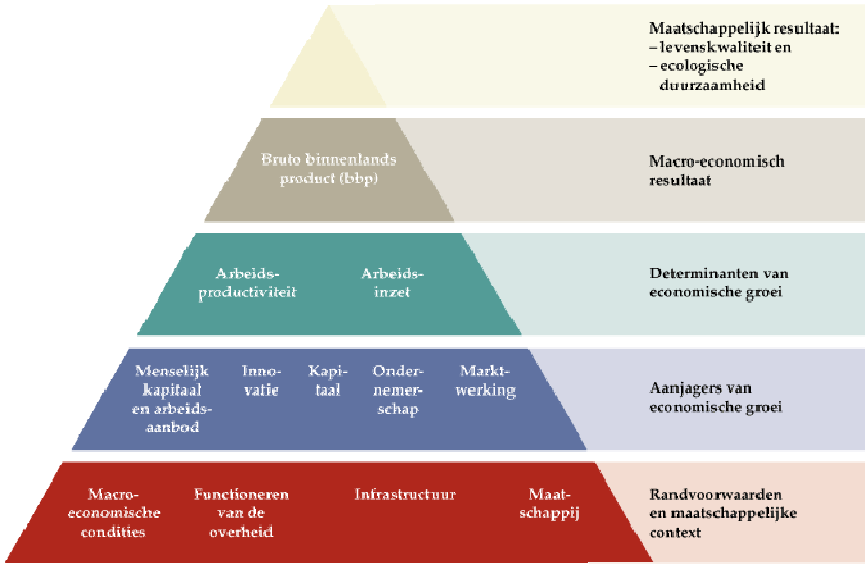
De afgelopen 15 jaar is veel (internationaal) onderzoek uitgevoerd naar de economische impact van investeringen in ICT. Uit deze onderzoeken blijkt onder andere dat sprake is van de volgende drie effecten van de ontwikkelingen op ICT-gebied op de economische groei:

- investeringen in ICT helpen de arbeidsproductiviteit te verhogen doordat werknemers efficiënter kunnen worden ingezet;
- snelle technologische ontwikkeling in de productie van ICT-goederen en diensten versterkt de efficiënte inzet van arbeid en kapitaal in de ICT-industrie zelf;
- het gebruik van ICT vergroot de efficiëntie van bedrijven, verlaagt transactiekosten en versnelt innovatie.

Het onderhavige onderzoek richt zich echter niet op de economische impact van investeringen in ICT in brede zin, maar specifiek op de *veiligheid en betrouwbaarheid* van de *ICT-infrastructuur*. Wat is het belang van die veiligheid en betrouwbaarheid voor de economische groei in Nederland?

De beschikbaarheid van een veilige en betrouwbare infrastructuur (weg, water, lucht, pijplijn en ICT) wordt in de economische theorie gezien als een belangrijke randvoorwaarde voor economische groei. Een onveilige en onbetrouwbare infrastructuur belemmert de marktwerking, de inzet en beschikbaarheid van het arbeidspotentieel, de innovatiekracht en daarmee de economische groei.

Figuur 2.2 Een conceptueel model van economische groei.



Bron: CBS

Gezien de relatief beperkte doorlooptijd en de brede vraag die aan het onderzoek ten grondslag lag, is er bij de start veel aandacht besteed aan de afbakening van het onderzoek.

Daarbij is in overleg met de opdrachtgever besloten het onderzoek te focussen op drie belangrijke elementen die bepalend zijn voor de bijdrage van een betrouwbare en veilige ICT-infrastructuur aan de duurzame economische groeikansen van Nederland:

2.2.1 De directe schade door veiligheids- en betrouwbaarheidsproblemen bij het bedrijfsleven in termen van productieverlies

Een onveilige en onbetrouwbare ICT-infrastructuur levert directe economische schade op bij het Nederlandse bedrijfsleven. Direct productieverlies, zoals de tijd die werknemers verliezen door spam, door virussen of door het down gaan van netwerken. Maar ook omzetverlies doordat verbindingen en informatiesystemen tijdelijk niet beschikbaar zijn. Daarnaast vergoeden bedrijven (bijvoorbeeld banken) de schade die hun klanten hebben geleden als gevolg van cybercrime activiteiten.

Het door ons uitgevoerde veldwerk was gericht op het in beeld brengen van het productieverlies. Andere elementen zijn meegenomen voor zover hier bestaande informatie over te vinden was uit eerder onderzoek (nationaal of internationaal). In de praktijk betekent dit dat wij in dit rapport geen inschatting maken van de totale directe economische schade. Hiervoor is nader onderzoek nodig.

2.2.2 De betekenis voor het vestigingsklimaat

Hoe belangrijk is een veilige en betrouwbare ICT-infrastructuur als vestigingsplaatsfactor? Op nationale schaal is dit vooral een relevante vraag voor bedrijven met een internationale oriëntatie: vestigen zij zich in Nederland of kiezen zij een ander land als vestigingsplaats? Blijven zij in Nederland of vertrekken zij? Bij het doen van uitspraken over het vestigingsklimaat is het vooral van belang om te kijken naar de relatieve positie van Nederland ten opzichte van andere concurrerende landen.

Belangrijke vraag is dan: hoe scoort Nederland wat betreft de veiligheid en betrouwbaarheid van de ICT-infrastructuur ten opzichte van deze landen. Daarbij staat de perceptie die bedrijven hebben centraal.

2.2.3 De (meer)waarde van vertrouwen in ICT bij de eindgebruiker (bedrijven en consumenten)

Een tweede belangrijk onderdeel van het onderzoek betreft de (meer)waarde van vertrouwen in de ICT-sector (specifiek in relatie tot veilige/betrouwbare netwerken en informatieveiligheid) bij eindgebruikers. De groeiende afhankelijkheid van ICT zorgt er voor dat veel bedrijven en consumenten een toenemende zorg hebben over de veiligheid van ICT. De mate waarin bedrijven en consumenten vertrouwen hebben in hun ICT-dienstverleners, evenals de manier van zakendoen en de veiligheid van de diensten en netwerkomgevingen van zakelijke relaties, wordt een steeds belangrijkere factor voor duurzame economische groei.

2.3 Definitie ICT-infrastructuur

In dit onderzoek wordt gekeken naar het belang van een veilige en betrouwbare *ICT-infrastructuur* voor de Nederlandse economie.

Daarbij definiëren wij de ICT-infrastructuur als:

Het geheel van de openbare datanetwerken en -verbindingen tussen organisaties en huishoudens (de basisinfrastructuur) en alle externe databases en informatiesystemen (van overheidsorganisaties, banken, klanten en leveranciers) waarmee organisaties of huishoudens data uitwisselen. Interne bedrijfs- en thuisnetwerken vallen buiten de reikwijdte van het onderzoek[5].

In dit onderzoek kijken wij naar twee onderdelen van ICT-infrastructuur:

- openbare datanetwerken en –verbindingen;
- externe databases en informatiesystemen die cruciaal zijn voor de continuïteit van de bedrijfsvoering van organisaties of een van maatschappelijk belang zijn.

Openbare datanetwerken en -verbindingen

Datanetwerken of -verbindingen zijn de voorzieningen die nodig zijn om digitale gegevens (data) te transporteren. Dit betreft alle technische middelen die het elektronische signaal als datadrager transporteren (fysieke faciliteiten), verdelen (netwerk switching) en routeren (netwerk routing). Het onderzoek richt zich daarmee op vaste en mobiele *datanetwerken*. Vaste en mobiele *spraaknetwerken* vallen (voor zover dit onderscheid te maken is) buiten het onderzoek.[6]

---

5 *De genoemde definitie vormt het uitgangspunt voor het onderzoek. Bij de interpretatie van de uitkomsten van het onderzoek dient er echter rekening mee gehouden te worden dat het begrip ICT infrastructuur niet duidelijk omlijnd is. Vaak is niet duidelijk waar ICT infrastructuur ophoudt en ICT toepassingen beginnen. Daarnaast kan een gebruiker van de infrastructuur niet altijd onderscheiden of problemen waarmee hij/zij geconfronteerd wordt te wijten zijn aan de externe ICT infrastructuur (bijv. een onveilige dataverbinding) of dat de problemen hun oorzaak vinden binnen het eigen interne netwerk.*

6 *Zo zijn er ook spraaktoepassingen via het internet mogelijk (Skype) en is voor eindgebruikers het onderscheid veelal niet duidelijk.*

Dit onderzoek richt zich specifiek op het 'openbare, digitale snelwegennet'. De veiligheid van bedrijfs- of thuisnetwerken valt buiten de scope van het onderzoek vallen. Vanuit het perspectief van veiligheid en betrouwbaarheid is de *aansluiting* van deze bedrijfs- en thuisnetwerken op het 'digitale snelwegennet' interessant. Dit punt vormde wel onderdeel van de scope van het onderzoek.

Databases en informatiesystemen

Bij een database of informatiesysteem gaat het om het elektronische opslagmedium van digitale gegevens (data) waaruit informatie kan worden opgevraagd door en worden gepresenteerd aan personen of systemen (bijvoorbeeld eindgebruikers, andere informatiebronnen, informatiesystemen of internetdiensten) via een datanetwerk of een gebruikersinterface. Wij beschouwen databases en informatiesystemen dus als een technisch functionerend systeem dat bedoeld is voor de opslag, bewerking en ontsluiting van digitale gegevens (data).

Niet alle informatiebronnen worden binnen dit onderzoek gezien als onderdeel van de Nederlandse ICT-infrastructuur. Bijvoorbeeld, databases en informatiesystemen die door bedrijven binnen hun interne netwerk gebruikt worden rekenen we hier niet onder. We beperken ons tot databases en informatiesystemen die toegankelijk en bedoeld zijn voor extern gebruik en van essentieel belang zijn voor een onverstoorde bedrijfsvoering van organisaties. Het gaat dan bijvoorbeeld om de (voor externen toegankelijkheden) databases en informatiesystemen van overheidsorganisaties (basisregistraties) en banken (betalingssystemen). De veiligheid en betrouwbaarheid van deze systemen is van groot belang voor de (perceptie van) de veiligheid en betrouwbaarheid van de totale Nederlandse ICT-infrastructuur.

2.4 Definitie veiligheid en betrouwbaarheid

Voor de definitie van veiligheid en betrouwbaarheid van de ICT-infrastructuur volgen wij de internationaal erkende kwaliteitsaspecten op dit terrein. Bij het begrip veiligheid en betrouwbaarheid van ICT maken we onderscheid in:

1 **Beschikbaarheid & continuïteit:** de mate waarin een datanetwerk en/of informatiebron in bedrijf is en onverstoord kan functioneren.
2 **Integriteit:** de juistheid, volledigheid, tijdigheid en controleerbaarheid van het functioneren van de ICT-infrastructuur.
3 **Exclusiviteit:** de mate waarin de toegang tot de ICT-infrastructuur beperkt is tot de groep van gerechtigden die hiertoe daadwerkelijk toegang nodig hebben.

ICT-infrastructuur is betrouwbaar als deze een aanvaardbaar niveau van dienstverlening (Quality of Service) kan blijven garanderen als (onbedoelde, opzettelijke, of natuurlijk veroorzaakte) fouten zich voordoen[7]. Dienstverlening is aanvaardbaar als deze voldoet aan de minimale eisen van de gebruiker in termen van de bovenstaande kwaliteitsattributen. Als de dienstverlening onder deze grens komt is deze niet aanvaarbaar.

[7] *Bron: Trust on infrastructure, ENIS, 2010*

Ook kan een optimaal niveau van dienstverlening worden onderkend, waarbij de verhouding niveau van dienstverlening en kosten optimaal is. Organisaties sluiten vaak Service Level Agreements (SLA's) af met netwerkleveranciers om een bepaalde Quality of Service te garanderen.

In Bijlage IV wordt nader ingegaan op hoe in het onderzoek de kwaliteitsaspecten voor datanetwerken en informatiebronnen zijn gehanteerd.

3 Directe schade bij bedrijven door ICT-problemen

3.1 Inleiding

In dit hoofdstuk staat de *directe* schade voor het Nederlands bedrijfsleven (inclusief de non-profit sector) centraal door ICT-problemen met een oorzaak buiten de organisatie.

In paragraaf 3.2 brengen wij allereerst de problematiek in beeld: Hoeveel bedrijven hebben jaarlijks last van ICT problemen die zijn veroorzaakt buiten de eigen organisatie? Om welke problemen gaat het dan?

Betrouwbaar cijfermateriaal over de jaarlijkse schade veroorzaakt door ICT-problemen van buiten de organisatie ontbreekt[8]. Bovendien is het lastig in beeld te brengen, aangezien het gaat om een breed begrip, waarbij het afbakenen van de definitie van het begrip 'schade' lastig is[9].

Ook dit onderzoek biedt geen totaalbeeld. Daarvoor zou een groter, meer omvattend onderzoek nodig zijn. Gegeven de omvang en doorlooptijd van ons onderzoek hebben wij ons in ons veldwerk gericht op informatie die al bekend is uit eerder onderzoek en is in het veldwerk de verdieping gezocht op twee belangrijke onderdelen: het productieverlies als gevolg van netwerkuitval en productieverlies als gevolg van spam (paragraaf 3.3).

Paragraaf 3.4 gaat in op de investeringen die bedrijven (eindgebruikers) in Nederland doen om ICT veiligheids- en betrouwbaarheidsproblemen tegen te gaan.

We sluiten het hoofdstuk af met een overzicht van de belangrijkste conclusies uit dit hoofdstuk (paragraaf 3.5).

De belangrijkste bron voor dit hoofdstuk vormt een webenquête die is uitgezet onder het panel van de ICT-barometer (gemiddeld 600 respondenten)[10].

---

8 *Zie ook Govcert, Trendrapport Cybercrime en Digitale Veiligheid, 15 november 2010*

9 *Zie o.a. NRC Handelsblad, Cybercrime even schadelijk als gewone diefstal, 5 januari 2011. In dit bericht wordt door Govcert een analyse gegeven van de reden waarom er zo weinig bekend is over de economische schade van cybercrime en digitale veiligheid.*

10 *De enquête biedt een inschatting van de respondenten over het voorkomen van ICT problemen binnen hun organisatie. Er is door ons geen (verder) gericht onderzoek uitgevoerd binnen de organisaties van de respondenten.*

Waar mogelijk hebben wij de uitkomsten van deze enquête vergeleken met gegevens die bekend zijn uit eerder onderzoek, om de plausibiliteit van de resultaten uit de enquête in te schatten en op punten aan te vullen.

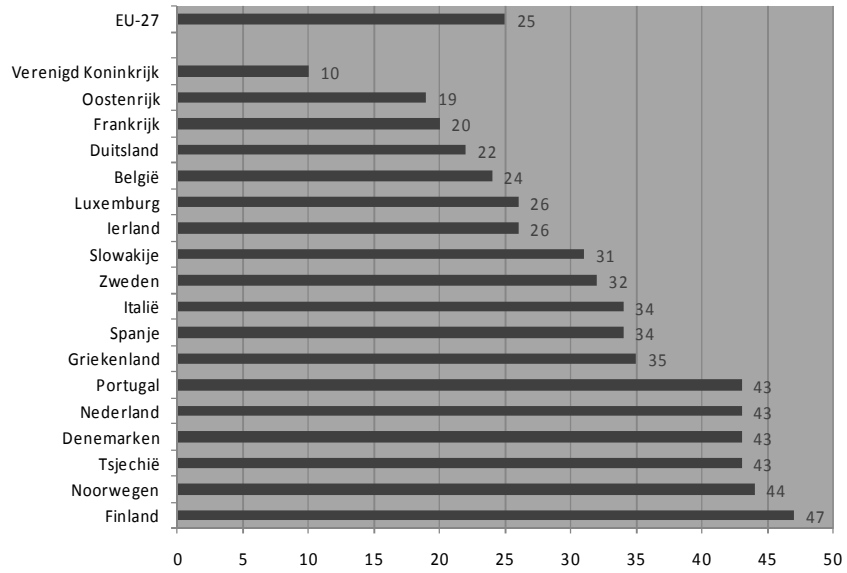
3.2 ICT-problemen

Bijna de helft van de Nederlandse grote bedrijven wordt jaarlijks getroffen door ICT beveiligingsincidenten

In Nederland werd in 2009 43% van de bedrijven van 250 werknemers of meer getroffen door een of meerdere ICT beveiligingsincidenten (zie Figuur 3.1). Daarbij ging het om:

- uitval als gevolg van storingen of door aanvallen van buitenaf;
- vernietiging of verminking van datadoor infectie of door ongeoorloofde toegang;
- onthulling van vertrouwelijke gegevens door inbraak, pharming of phishing.

Figuur 3.1 % grote bedrijven getroffen door ICT-beveiligingsincidenten, 2009.



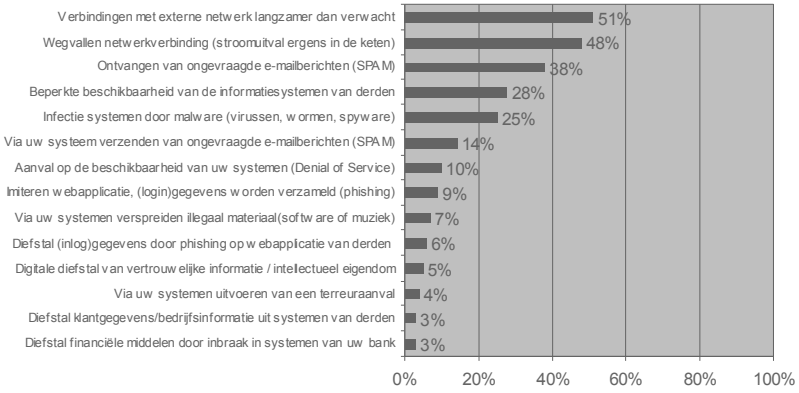
Bron: Eurostat- bedrijven van 250 werknemers en meer, excl. de financiële sector

Vergeleken met de ons omringende landen is het aandeel bedrijven met ICT-beveiligingsincidenten hoog. Nederland behoort met Denemarken en Noorwegen tot de landen met meeste bedrijven die werden getroffen door ICT-beveiligingsincidenten. De Europese koploper is Finland, met 47 procent. Het CBS, dat de cijfers voor Nederland publiceerde, concludeert dat de landen met naar verhouding veel van deze incidenten zich kenmerken door relatief veel en geavanceerd ICT-gebruik. Een gevolg hiervan is dat het risico op incidenten ook groter is[11].

11 *Bron: CBS, Webmagazine 5 januari 2011, Veel incidenten ICT-beveiliging bij bedrijven.*

Trage of uitvallende netwerkverbinding meest voorkomende ICT-probleem
In Figuur 3.2 is weergegeven met welke problemen bedrijven in Nederland te maken hebben gehad in de periode oktober 2009-oktober 2010. Uit de figuur komt naar voren dat de helft van de bedrijven in het afgelopen jaar een of meer keer te maken hebben gehad met een tragere externe netwerkverbinding of met het helemaal wegvallen van de externe netwerkverbinding. Bijna 40% van het panel van de ICT-barometer zegt het afgelopen jaar last te hebben ondervonden door spam. Het gaat hierbij om ongewenste e-mailberichten die niet zijn afgevangen door spamfilters. Volgens een periodiek onderzoek door Symantec schommelt het percentage ongewenste e-mailberichten het afgelopen jaar rond de 80% tot 95% van alle verstuurde e-mailberichten[12]. Ongeveer een kwart van de respondenten heeft te maken gehad met de uitval van (belangrijke) informatiesystemen van derden en een infectie van het systeem door malware of virussen.

Figuur 3.2 % Nederlandse bedrijven dat tussen oktober 2009 en oktober 2010 last heeft gehad van de onderstaande ICT-problemen.



Bron: ICT-barometer, Ernst & Young, 2010.

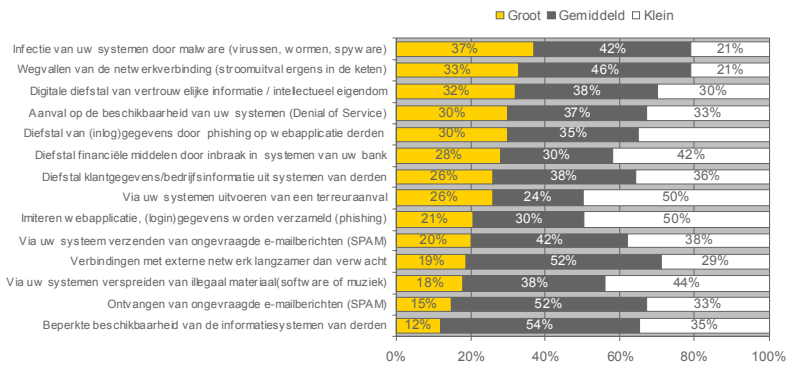
Infectie door malware, wegvallen netwerkverbinding en informatiediefstal problemen met de hoogste potentiële impact op de bedrijfsvoering
ICT-problemen die vaak voorkomen hoeven niet per se ook veel economische schade te veroorzaken. Bijvoorbeeld doordat de bedrijfsprocessen vrijwel ongehinderd door blijven draaien. Andersom kunnen ICT-problemen die niet vaak voorkomen wel veel schade veroorzaken wanneer ze zich voordoen.

Van de in hoofdstuk 2 gedefinieerde veiligheids- en betrouwbaarheidsaspecten worden vooral de bescherming tegen onbevoegd gebruik van gegevens (72%) en de beschikbaarheid en continuïteit van verbindingen en informatiebronnen (62%) als belangrijk ingeschat voor de eigen organisatie. Andere aspecten zoals de juiste en volledige overdracht van informatie, de tijdige overdracht van informatie en de controleerbaarheid van de ICT-infrastructuur worden door minder respondenten als belangrijk voor de organisatie beschouwd.

Uit Figuur 3.3 komt een zelfde beeld naar voren. Het wegvallen van de netwerkverbinding en de infectie van systemen door malware zijn behalve veel voorkomende ICT-problemen, ook problemen met een grote potentiële impact op de bedrijfsvoering. De diefstal van vertrouwelijke gegevens, een denial of service aanval en phishing worden (wanneer zij voorkomen) ook gezien als problemen met een grote impact op de bedrijfsvoering.

12 *Bron: State of spam & Phishing #47, Symantec, november 2010.*

Figuur 3.3 Inschatting van de potentiële impact van de belangrijkste ICT-problemen op de bedrijfsvoering.



Bron: ICT-barometer, Ernst & Young, 2010.

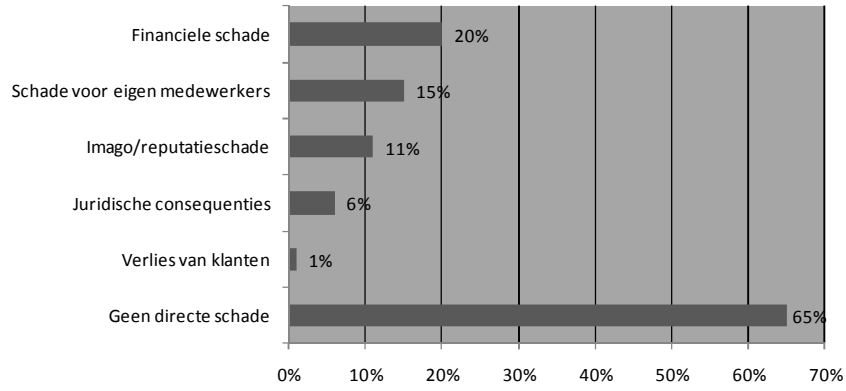
3.3 Directe schade door ICT problemen van buitenaf

In deze paragraaf staat de directe schade die bedrijven ondervinden als gevolg van ICT problemen van buitenaf centraal. het productieverlies als gevolg van netwerkuitval en als gevolg van het ontvangen en verwerken van spam-berichten centraal. We gaan daarbij eerst in op de schade door cybercrime en kijken vervolgens dieper naar de directe schade in termen van productieverlies als gevolg van spam.

3.3.1 Directe schade van cybercrime

Een op de drie bedrijven in Nederland leidt directe schade door cybercrime
Uit onderstaande figuur blijkt dat een op de drie organisaties directe schade ondervindt als gevolg van cybercrime. Bij 20% van de organisaties gaat het om directe financiële schade. Ook de schade voor eigen medewerkers (bijvoorbeeld de tijd die gemoeid is met schadeherstel) en imagoschade worden regelmatig genoemd. Vooral grote bedrijven ondervinden directe schade. Bijna de helft van de ondernemingen van 500 werknemers of meer heeft schade opgelopen.

Figuur 3.4 % organisaties dat in het afgelopen jaar schade heeft ondervonden van cybercrime, naar type schade.



Bron: Cybercrime, ICT-barometer, Ernst & Young, februari 2011.

In de Cybercrime ICT-barometer van maart 2011 is tevens aan de respondenten gevraagd om een inschatting te maken van de omvang van de directe financiële schade (dus los van eventuele schade in termen van de tijd die nodig is voor schadeherstel, imagoschade of andere schade) die zij hebben geleden.

De bedrijven die aangeven directe financiële schade te hebben ondervonden als gevolg van cybercrime (20% van het totaal) geven hierover het volgende aan:

- 34% geeft aan directe financiële schade te hebben geleden van minder dan € 10.000;
- 53% geeft aan directe financiële schade te hebben geleden van minimaal € 10.000 tot € 500.000;
- 13% van de organisaties geeft schadebedragen aan van € 1.000.000 of meer.

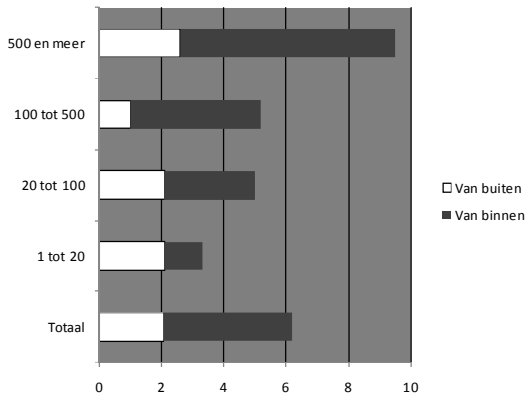
In het onderzoek zijn de uitkomsten niet geëxtrapoleerd naar een schadebedrag voor de hele Nederlandse economie. Wel is duidelijk dat de schade zeer aanzienlijk is.

3.3.2 Derving in arbeidstijd door uitval van het netwerk

Gemiddeld 6 keer per jaar netwerkuitval, waarvan 2 keer door oorzaken van buitenaf

De bedrijven van de respondenten uit de ICT-barometer hebben in de 12 maanden voor het invullen van de vragenlijst gemiddeld 6 maal per jaar een ICT-probleem waardoor de werking van het netwerk voor werknemers beperkt of geheel verhinderd is. Met de bedrijfsomvang neemt ook het aantal malen dat sprake is van uitval toe. Uit Figuur 3.5 blijkt dat bij de bedrijven van 500 werknemers en meer in het afgelopen jaar gemiddeld bijna 10 keer sprake is geweest van ICT-problemen, waardoor de werking van het netwerk beperkt of geheel gehinderd was. Bij bedrijven tot 20 werknemers was dit gemiddeld ongeveer 3 keer[13].

Figuur 3.5 Aantal maal in de afgelopen 12 maanden dat er ICT-problemen zijn opgetreden waardoor de werking van het netwerk voor werknemers beperkt of geheel verhinderd was.



Bron: ICT-barometer, Ernst & Young, 2010.

In gemiddeld tweederde van de gevallen ging het om oorzaken binnen de organisatie zelf, in één derde van de gevallen lag de oorzaak buiten de organisatie. In absolute aantallen: De bedrijven van de respondenten uit de ICT-barometer hadden in de 12 maanden voorafgaand aan het onderzoek gemiddeld twee maal een ICT-probleem van buiten de organisatie waardoor het netwerk niet of maar beperkt werkte[14].

---

13 *In de ICT barometer worden andere klassen gebruikt voor de indeling van de omvang van organisaties dan in onderzoek van CBS en van Eurostat.*

14 *Ter vergelijking: een huishouden in Nederland wordt gemiddeld eenmaal per 3 jaar getroffen door een stroomstoring. Een gemiddeld huishouden in Nederland wordt*

Uit Figuur 3.5 komt naar voren dat er tussen kleine en grote bedrijven uit de ICT-barometer weinig verschil bestaat in het aantal maal dat de werking van het netwerk gehinderd was door oorzaken van buitenaf. Bij grote bedrijven (500 werknemers en meer) is de uitval door oorzaken van buitenaf daardoor relatief beperkter dan bij kleine bedrijven (1 tot 20 werknemers).

Per keer duurt het 100 minuten om het netwerkprobleem te verhelpen
Het duurde bij de organisaties uit de ICT-barometer gemiddeld 100 minuten per incident voor de werking van het netwerk weer hersteld was. Bij de organisaties met minder dan 20 werknemers duurde het gemiddeld het langst (113 minuten). Bij de organisaties met 100 tot 500 werknemers het kortst (76 minuten). Een verklaring voor dit verschil is mogelijk gelegen in het gespecialiseerde personeel dat bij grotere bedrijven aanwezig is om de problemen op te lossen. Bij kleine bedrijven is dergelijk personeel in veel gevallen niet aanwezig. Tussen de verschillende sectoren zijn de verschillen beperkt.

Productieverlies voor netwerkuitval door oorzaken buiten de organisatie naar schatting 100 tot 150 miljoen euro
Op basis van het bovenstaande is het mogelijk om een globale inschatting te maken van de derving in arbeidskosten door netwerkuitval.

Daarbij hanteren we de volgende veronderstellingen:

- Iedere organisatie in Nederland heeft jaarlijks gemiddeld 6 maal te maken met vertraging of uitval van het netwerk waardoor de toegang voor werknemers beperkt of geheel verhinderd is. Gemiddeld 2 maal per jaar gaat het om incidenten met een oorzaak buiten de organisatie (zie figuur 3.3).
- Per incident kost het gemiddeld 100 minuten om het probleem te verhelpen (zie hierboven).
- Niet iedere werknemer heeft even veel last van vertraging of uitval van het netwerk aangezien niet iedere werknemer even ICT-gerelateerd werk doet. Uit onderzoek van het Sociaal Cultureel Planbureau uit 2005 blijkt dat Nederlandse werknemers gemiddeld ongeveer de helft van hun werktijd computerwerk uitvoeren[15]
- Niet al het computerwerk is even netwerkafhankelijk. Bepaalde vormen van computerwerk kunnen ook doorgaan wanneer het netwerk tijdelijk uitvalt. Ander computerwerk is volledig afhankelijk van toegang tot het netwerk. Wij hebben geen bronnen kunnen vinden van de mate van netwerk afhankelijkheid van het computerwerk. Wij nemen voor onze schatting aan dat de 40 tot 60 procent van het computerwerk in Nederland netwerkafhankelijk is.
- Het totale arbeidsvolume in Nederland bedraagt 6,7 miljoen fte[16].
- We gaan uit van gemiddelde arbeidskosten van 25 euro per uur per werknemer.

In Tabel 3.1 is op basis van deze veronderstellingen een inschatting uitgewerkt van de gederfde arbeidskosten als gevolg van netwerkuitval. In de tekst werken we de redenering uit voor de incidenten met een oorzaak van buitenaf aangezien die vanuit de afbakening van het onderzoek het meest relevant is.

---

gemiddeld eenmaal per 204 jaar getroffen door een gasstoring (bron: KEMA/Kiwa Gas technology).

15 *Bron: Verzonken Technologie, ICT en de arbeidsmarkt, SCP, juni 2005.*

16 *Bron: CBS*

Wanneer per organisatie gemiddeld tijdens kantooruren 2 incidenten zijn met een oorzaak van buitenaf plaatsvinden en het per incident gemiddeld 100 minuten duurt voor dit is opgelost, ligt het netwerk door ICT-problemen van buiten per organisatie jaarlijks gemiddeld 200 minuten stil. Uitgaande van de bovenstaande veronderstellingen kan de gemiddelde (fulltime) werknemer dan jaarlijks naar schatting 40 tot 60 minuten (200 minuten * 50% * (40% tot 60%)) niet of beperkt werken door ICT-problemen van buiten de organisatie. Uitgaande van een totaal arbeidsvolume in Nederland van 6,7 miljoen fte en gemiddelde arbeidskosten van 25 euro per uur zou dit een jaarlijkse kostenpost voor het Nederlandse bedrijfsleven bedragen in de orde van grootte van 100 tot 150 miljoen euro aan derving in arbeidsuren (afgerond).

Tabel 3.1 Schatting gederfde arbeidskosten als gevolg van ICT-problemen waardoor de werking van het netwerk voor werknemers beperkt of geheel verhinderd was.

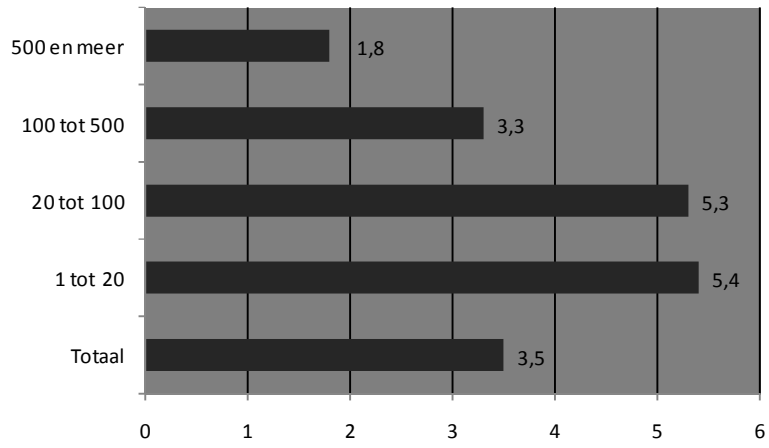
	Totaal	Door oorzaken van buiten
Gemiddeld aantal incidenten per organisatie	6	2
Aantal minuten geen of beperkte toegang tot netwerk	600 minuten	200 minuten
Gederfde arbeidstijd per fulltime werknemer	120 tot 180 minuten	40 tot 60 minuten
Gederfde arbeidskosten	300-450 mln. euro	100-150 mln. euro

3.3.3 Derving in arbeidstijd door spam

De gemiddelde werknemer is 3,5 minuut per dag bezig met de verwerking van spamberichten

De respondenten van de ICT-barometer schatten in dat zij gemiddeld 3,5 minuten per werkdag bezig zijn met de verwerking van spamberichten in hun mailbox. Dat is 17,5 minuut per week. Uitgaande van netto 47 werkweken per jaar is dat 822 minuten per jaar, of wel 13,7 uur per werknemer per jaar.

Figuur 3.6 Aantal minuten per werkdag dat respondenten kwijt zijn aan het verwerken van spam, naar bedrijfsomvang.



Bron: ICT-barometer, Ernst & Young, 2010.

Daarbij bestaan grote verschillen tussen grote en kleine bedrijven. Daar waar respondenten van grote bedrijven schatten dat zij gemiddeld 1,8 minuut per dag

besteden aan spam, is dat bij kleine bedrijven 5,4 minuten per dag. In het onderzoek is niet gevraagd naar de oorzaken van de verschillen.
Een plausibele verklaring lijkt echter dat grote bedrijven adequatere spamfilters hebben dan kleine bedrijven.

Schatting van de derving in arbeidskosten door spam
Met bovenstaande gegevens is het mogelijk om een globale inschatting te maken van de derving in arbeidkosten bij het Nederlandse bedrijfsleven als gevolg van spam.

We gaan bij onze inschatting uit van de volgende veronderstellingen:

- Eerste veronderstelling is dat alle werknemers binnen een organisatie die computerwerk doen per week evenveel tijd kwijt zijn met de verwerking van spamberichten. Wij achten deze veronderstelling plausibel aangezien de hoeveelheid spam niet afhankelijk is van de intensiteit van het computerwerk, noch van het aantal uren dat gewerkt wordt (ook bij afwezigheid vult de mailbox zich).
- Tweede belangrijke veronderstelling is dat de respondenten van de ICT-barometer op het terrein van spam niet afwijken van de gemiddelde computerwerknemer in Nederland[17].
- 50% tot 80% van de werknemers maakt een deel van hun werktijd gebruik van de computer[18]. Dat zijn 3,8 tot 6 miljoen werknemers die computerwerk verrichten.

Uitgaande van 25 euro aan gemiddelde arbeidskosten per uur voor de werkgever ligt de geschatte jaarlijkse derving in arbeidskosten voor het Nederlandse bedrijfsleven dan naar schatting 1 tot 2 miljard euro per jaar (afgerond, 4 tot 6 miljoen werknemers x 13,7 uur per jaar x 25 euro), ofwel grofweg 150 tot 300 euro per werknemer per jaar.
Vergelijking met ander onderzoek
In de afgelopen jaren zijn er met enige regelmaat inschattingen gemaakt van de economische schade door spam. Zo schatte McAfee het productiviteitsverlies per werknemer in 2009 in op 181 dollar per werknemer per jaar[19].
Onderzoeksbureau Ferris Research becijferde dat spam werkgevers in 2005 op jaarbasis 161 euro per werknemer kost. Ook duidelijk hogere bedragen worden genoemd. Zo becijferde Nucleus Research het productiviteitsverlies als gevolg van spam in 2007 op 712 dollar per werknemer per jaar. De 150 tot 300 euro per werknemer die uit ons onderzoek naar voren komt ligt daar tussenin.

17 *Ook dit achten wij een plausibele veronderstelling. De verschillen in het aantal minuten verwerkingstijd van spam tussen sectoren zijn klein. Na herweging van de uitkomsten naar de structuur van de Nederlandse werkgelegenheid naar organisatieomvang komt de gemiddelde verwerkingstijd voor spam ook uit op 3,5 minuten per dag.*

18 *Het SCP schat in haar onderzoek 'Verzonken Technologie, ICT en de arbeidsmarkt' uit 2005 het aandeel in op 80%. Om redenen van voorzichtigheid gaan wij in voor onze berekening uit van 50 tot 80 procent.*

19 *Bron: McAfee Research report, March 2009 spam Report*

3.3.4 Directe schade bij banken als gevolg van phishing en skimming

Schade skimming neemt af, schade phishing neemt toe

In de voorgaande paragrafen hebben wij ingezoomd op de derving in arbeidskosten bij het Nederlandse bedrijfsleven als gevolg van problemen met het netwerk en als gevolg van spam. Dit is een belangrijk aspect van de schade die bedrijven ondervinden als gevolg van veiligheidsproblemen in de ICT-infrastructuur, maar zeker niet het enige. Een belangrijk ander aspect is bijvoorbeeld de omzetschade die bedrijven ondervinden als gevolg van het tijdelijk niet beschikbaar zijn van hun website als gevolg van veiligheidsincidenten of de schade die banken vergoeden aan hun klanten wanneer zij worden getroffen door skimming of door phishingincidenten.

De gegevens die beschikbaar zijn om enig zicht te krijgen op de totale omvang en ontwikkeling van de economische schade voor bedrijven als gevolg van ICT-veiligheidsproblemen zijn zeer beperkt.

- Voor Nederland hebben wij alleen recente gegevens kunnen achterhalen over de directe schade bij Nederlandse banken als gevolg van phishing. Uit cijfers van de NVB blijkt dat de door banken in Nederland aan klanten vergoede schade als gevolg van fraude met internetbankieren (o.a. phishing) in 2009 op 1,9 miljoen euro lag. In 2010 komt deze schade duidelijk hoger uit. In de eerste helft van 2010 was de vergoede schade reeds opgelopen tot 4,3 miljoen euro. Hoewel de toename sterk is, gaat het vooralsnog om een zeer beperkt deel van de totale omvang van alle online-bancaire transacties.

De fraude met gekloonde pinpassen lijkt af te nemen. In 2009 werd voor 36 miljoen euro gefraudeerd met gekloonde pinpassen (skimming). In de eerste helft van 2010 lag de schade volgens de NVB op 11,8 miljoen euro.

3.4 Investeringen in ICT-veiligheid en –betrouwbaarheid

Hierboven is ingegaan op de schade die bedrijven ondervinden als gevolg van de veiligheids- en betrouwbaarheidsproblemen met de ICT infrastructuur. Bedrijven plegen investeringen om deze problemen te voorkomen en de veiligheid en betrouwbaarheid te vergroten. In deze paragraaf gaan we hier nader op in[20].

Zeventien procent van het ICT-budget ingezet voor borging veiligheid en betrouwbaarheid ICT

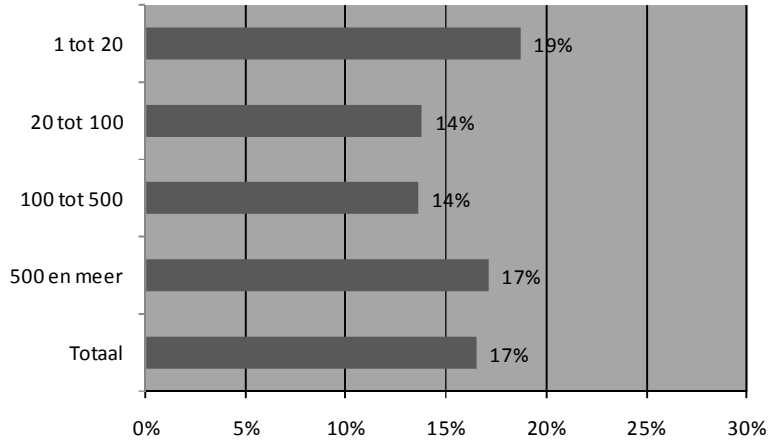
Bij de bedrijven die deelnemen aan de ICT-barometer wordt in 2010 gemiddeld 17% van het ICT-budget ingezet voor de borging van de veiligheid en betrouwbaarheid van de ICT[21]. Uit Figuur 3.7 blijkt dat kleine bedrijven (minder dan 20 werknemers) en grote bedrijven (meer dan 500 werknemers) het aandeel dat ingezet wordt voor veiligheid en betrouwbaarheid iets hoger inschatten dan de middelgrote bedrijven (20-100 werknemers).

---

20 *Het betreft de investeringen van in ICT-veiligheid en betrouwbaarheid door het bedrijfsleven (als eindgebruiker), dus exclusief de investeringen van consumenten, netwerk serviceproviders en de overheid.*

21 *Er zijn hierbij vrijwel geen verschillen in de inschatting van respondenten met en zonder ICT taken.*

Figuur 3.7 Aandeel van het ICT-budget dat wordt besteed aan veiligheid en betrouwbaarheid van ICT.

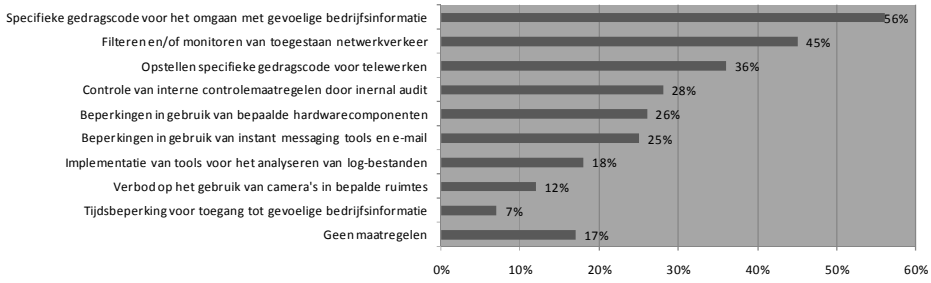


Bron: ICT-barometer, Ernst & Young, 2010.

De uitkomsten van ons onderzoek lopen sterk uiteen met de uitkomsten van de jaarlijkse Computer Crime and Security survey die het Amerikaanse Computer Security Institute jaarlijks uitvoert. Uit dit onderzoek blijkt dat in 2008 53% van de (Amerikaanse) bedrijven minder dan 5% van hun ICT budget uitgaven aan wat zij noemen: 'Information Security'[22]. Het grote verschil kan voortkomen uit een verschil in definitie. Daar waar CIS zich richt op informatieveiligheid, is in de ICT-barometer breed gevraagd naar de uitgaven aan veiligheid en betrouwbaarheid van ICT.

Uit Figuur 3.8 blijkt dat het uitlekken van bedrijfsgevoelige informatie vooral wordt bestreden door gedragscodes voor het omgaan met gevoelige informatie, het filteren en monitoren van netwerkverkeer en gedragscodes voor telewerken.

Figuur 3.8 Maatregelen om te voorkomen dat gevoelige bedrijfsinformatie uitlekt.

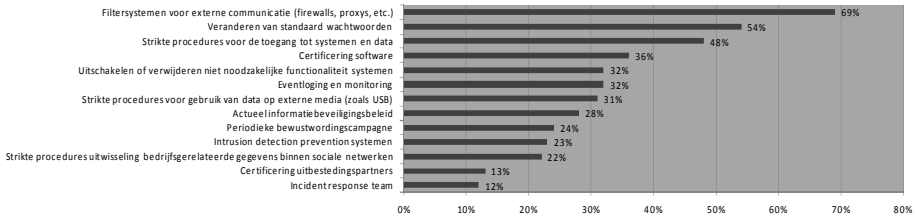


Bron: Cybercrime, ICT-barometer, Ernst & Young, februari 2011.

Filtersystemen, wachtwoord protocollen en toegangsprocedures voor systemen en data vormen de meest gehanteerde technische maatregelen van bedrijven om cybercrime tegen te gaan. Het gaat hierbij om basisvoorzieningen. Opvallend is dat deze basisvoorzieningen toch door een belangrijk deel van de bedrijven niet worden gebruikt.

22 *Bron: Computer Crime and Security Survey, CSI, 2008.*

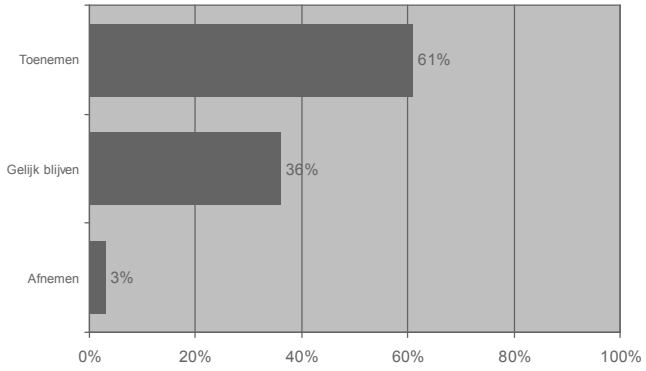
Figuur 3.9 Technische en procedurele maatregelen om cybercrime activiteiten te voorkomen of te detecteren.



Bron: Cybercrime, ICT-barometer, Ernst & Young, februari 2011.

Zoals Figuur 3.10 laat zien is de algemene tendens dat organisaties (61%) denken dat het belang van veilige en betrouwbare ICT-infrastructuur zal toenemen. De verwachting is dat de investering in ICT-veiligheid en –betrouwbaarheid zal toenemen.

Figuur 3.10 Het toenemen/gelijkblijven/afnemen van het belang van veilige en betrouwbare ICT-infrastructuur voor organisaties de komende vijf jaar.



Bron: ICT-barometer, Ernst & Young, 2010.

3.5 Conclusie

Het borgen van de beschikbaarheid en continuïteit van verbindingen en informatiebronnen en de bescherming tegen onbevoegd gebruik van gegevens zijn voor Nederlandse bedrijven de twee belangrijkste aandachtspunten voor bedrijven op het terrein van ICT veiligheid en betrouwbaarheid.

Bijna de helft van de Nederlandse bedrijven (43%) wordt op jaarbasis getroffen door ICT-veiligheidsincidenten (inclusief uitval van ICT als gevolg van storingen). Dat is duidelijk meer dan in de meeste andere Europese landen.

Het wegvallen van de netwerkverbinding en de infectie van systemen door malware zijn veel voorkomende ICT-problemen, met volgens bedrijven een grote potentiële impact op de bedrijfsvoering. De diefstal van vertrouwelijke gegevens, een denial of service aanval en phishing komen veel minder vaak voor, maar worden (wanneer zij voorkomen) ook gezien als problemen met een grote impact op de bedrijfsvoering.

Maar wat is de economische waarde van de directe schade die bedrijven ondervinden als gevolg van ICT-veiligheidsincidenten? Of in termen van kansen: welke kostenbesparingen zijn mogelijk bij het Nederlandse bedrijfsleven wanneer de betrouwbaarheid en de veiligheid van de ICT infrastructuur op een hoger peil wordt gebracht?

Deze vraag is lastig te beantwoorden aangezien het om een zeer breed begrip gaat en ook het begrip schade niet eenvoudig te definiëren is. Dit onderzoek geeft een globale inschatting op een beperkt aantal onderdelen. Voor het verkrijgen van het meer gedetailleerd beeld is aanvullend onderzoek nodig.

Uit onderzoek van Ernst & Young naar cybercrime komt naar voren dat één op de drie bedrijven schade heeft ondervonden als gevolg van cybercrime. Een op de vijf bedrijven leed hierdoor ook directe financiële schade. De omvang van deze financiële schade is aanzienlijk.

In het onderzoek is verder ingezoomd op twee directe schadeposten voor het bedrijfsleven:

- het productieverlies als gevolg van netwerkuitval;
- het productieverlies als gevolg van ontvangen en verwerken van spam.

Uit Tabel 3.2 blijkt dat vooral de derving van arbeidskosten van het lezen en verwerken van spam een belangrijke schadepost betekent voor het Nederlandse bedrijfsleven. Wij schatten deze schadepost voor 2010 in op 1 tot 2 miljard euro. Dat is 150 tot 300 euro per werknemer per jaar. Vermindering van de tijd die werknemers nodig hebben voor de verwerking van spam kan het Nederlands bedrijfsleven (macro) dus een behoorlijke besparing opleveren. Opvallend is dat spam door bedrijven wel gezien wordt als een veel voorkomend probleem, maar niet als een probleem dat een grote impact heeft op de bedrijfsvoering. Vooral binnen kleinere bedrijven zijn werknemers per dag relatief veel tijd kwijt met de verwerking van spamberichten.

Tabel 3.2 Overzicht globale inschatting productieverlies in Nederland als gevolg van netwerkuitval en spam – 2010

	Door oorzaken van buiten de eigen organisatie	Door oorzaken binnen de eigen organisatie
Productieverlies door netwerkuitval	100-150 mln euro	200-300 mln. euro
Productieverlies als gevolg van spam	1 – 2 mld. euro	N.v.t.
Totaal productieverlies als gevolg van netwerk-uitval en spam	**1,1 – 2,2 mld. euro**	**0,2 – 0,3 mld. Euro**

In het onderzoek hebben wij ingezoomd op twee schadeposten. Andere belangrijke schadeposten zoals de schade door digitale diefstal van vertrouwelijke informatie (klantgegevens, inlogcodes, bedrijfsgegevens), het omzetverlies bij bedrijven als gevolg van het tijdelijk niet beschikbaar zijn van de website en de schade als gevolg van diefstal van vertrouwelijke informatie zijn niet verder uitgewerkt in het onderzoek. Er is niet voldoende informatie bekend om (binnen dit onderzoek) tot een goede inschatting te komen van de omvang van deze schadeposten. Bekend is wel dat de schade voor financiële instellingen als gevolg van fraude met internetbankieren (o.a. phishing) in de eerste helft van 2010 volgens de banken 4,3 mln. euro bedroeg. Ook cascade-effecten (door de toenemende verknoping van netwerken en de toenemende afhankelijkheid van de economie van ICT) zijn buiten beschouwing gelaten. Om het beeld over de omvang van de schade verder in te vullen is verder onderzoek nodig.

Bedrijven doen ook investeringen om ICT veiligheids- en betrouwbaarheids-problemen te voorkomen. Uit ons onderzoek komt naar voren dat bedrijven en non-profitorganisaties in 2010 gemiddeld 17 procent van hun totale ICT-budget besteden aan ICT veiligheid[23].

23 *Daarnaast doen ook consumenten, de netwerkserviceproviders en de overheid investeringen om de ICT veiligheid te verhogen. Deze zijn in dit onderzoek niet in beeld gebracht.*

4 Vertrouwen bij de eindgebruiker

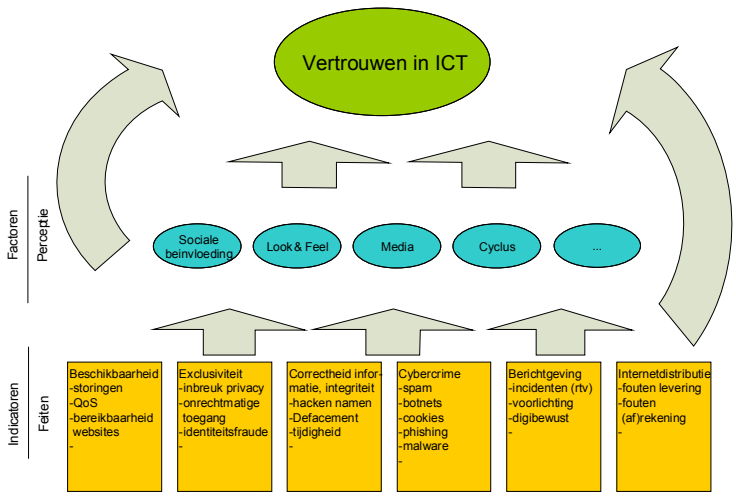
4.1 Inleiding

Het gebruik van de ICT-infrastructuur is niet meer weg te denken uit de hedendaagse samenleving. De afhankelijkheid van telefoons, computers en internet is zo groot geworden, dat organisaties niet meer kunnen functioneren zonder het gebruik van ICT. Het overgrote deel van de betalingen gebeurt via geautomatiseerde betalingssystemen. De verkoop van producten en diensten via het internet groeit jaar op jaar.

In het vorige hoofdstuk zijn we ingegaan op de ICT problemen die bedrijven ondervinden. Het ging daarbij om de feitelijke problemen. In dit hoofdstuk staat het vertrouwensaspect centraal. De mate waarin bedrijven en consumenten vertrouwen hebben in de ICT infrastructuur is bepalend voor het gebruik van de ICT infrastructuur en daarmee voor de economische waarde die gecreëerd wordt via die infrastructuur.

In Figuur 4.1 is een door TNO ontwikkeld model weergegeven dat in beeld brengt hoe het vertrouwen in ICT bij eindgebruikers tot stand komt. De figuur laat zien dat bij het vertrouwen naast feiten en eigen ervaringen ook perceptie een belangrijke rol speelt. Deze perceptie wordt beïnvloed door onder andere berichtgeving in de media en door sociale beïnvloeding, maar ook door de look & feel van de aangeboden diensten.

Figuur 4.1 Van feiten naar vertrouwen, het belang van de perceptie



Bron: TNO, 2010

We hanteren in dit hoofdstuk een brede definitie van vertrouwen in ICT. Daarin spelen verschillende zaken een rol, zoals privacyaspecten en het vertrouwen dat betalingen elektronische transacties veilig kunnen plaatsvinden, maar bijvoorbeeld ook het vertrouwen in de levering van goederen of diensten door internetwinkels.

4.2 Vertrouwen bij het bedrijfsleven

4.2.1 Gebruik van de ICT infrastructuur door het Nederlandse bedrijfsleven

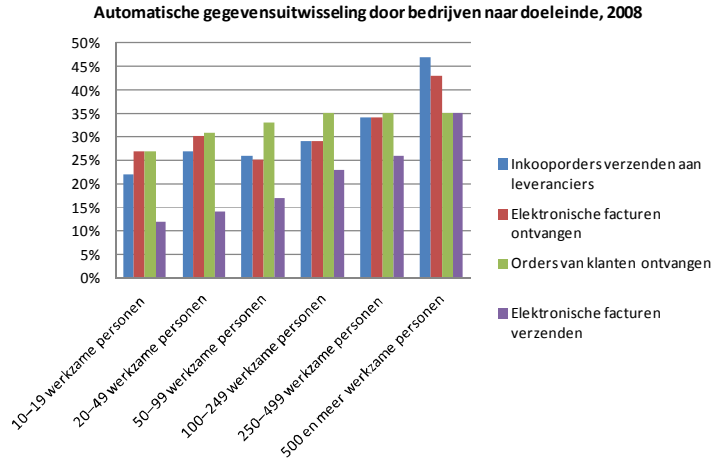
Bijna alle Nederlandse bedrijven maken gebruik van internet

In januari 2009 heeft 96% van de Nederlandse bedrijven een internetaansluiting, waarvan 84% een eigen internetpagina heeft. Daarmee onderscheidt Nederland zich overigens niet, want bijna alle Europese landen hebben een hoge internetgraad als het gaat om bedrijven[24].

Bedrijven maken gebruik van internet en openbare netwerken voor een diversiteit aan activiteiten, zoals plaatsen en ontvangen van orders, het ontvangen en verzenden van facturen, gegevensuitwisseling met overheden en financiële instellingen, e-mailverkeer, faciliteren van thuiswerken, ontsluiting van de eigen website, klantenservice, adverteren, werving van personeel, tracking & tracing van logistieke processen, gebruik van social media voor marketing en monitoring doeleinden en het buiten de deur plaatsen van servers.[25]

Binnen Nederland maken grote bedrijven meer gebruik van internet dan het midden- en kleinbedrijf. Bijvoorbeeld, als het gaat om het hebben van een eigen internetpagina, dan geldt dat voor 96% van de grote bedrijven (meer dan 249 medewerkers), en maar voor 82% van kleine bedrijven (10 tot 49 medewerkers)[26]. Ook voor het uitwisselen van gegevens maken grote bedrijven meer gebruik van internet en openbare datanetwerken dan middengrote en kleine bedrijven (zie Figuur 4.2).

Figuur 4.2 Gebruik van ICT-infrastructuur door bedrijven voor gegevensuitwisseling.



Bron: ICT-gebruik bedrijven, CBS, 2008.

---

24 *Bron: ICT usage in enterprises 2009, Eurostat, Data in focus, 1/2010.*

25 *Bronnen: De digitale economie 2009, CBS; ICT usage in enterprises 2009, Eurostat, Data in focus, 1/2010; ICT-gebruik bedrijven, CBS, 2008*

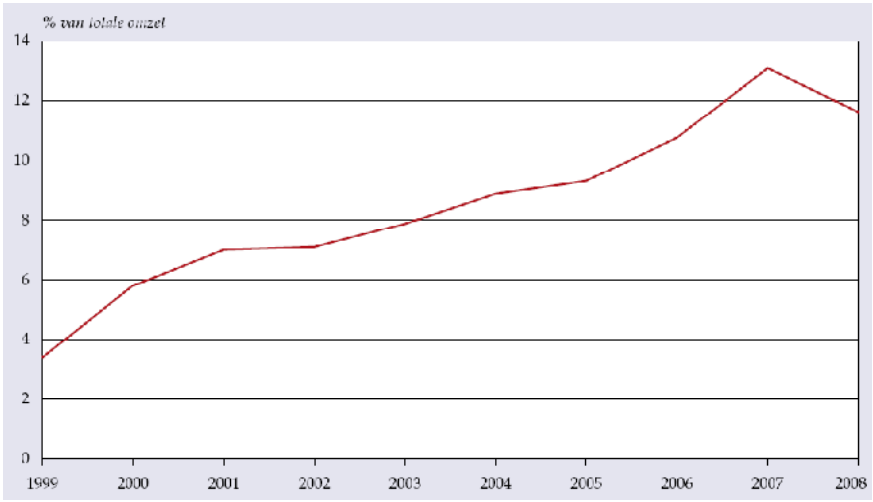
26 *Bron: Enterprises - Computers: Devices and communication systems (NACE Rev. 2), Eurostat, 09-09-2010.*

Internet is een groeiend verkoopkanaal voor Nederlandse bedrijven
In 2008 maakte ongeveer 25% van de Nederlandse bedrijven gebruik van internet voor het ontvangen van orders[27]. Daarmee loopt Nederland in Nederland voorop samen met Tsjechië, Denemarken en Duitsland. In Noorwegen ligt het aandeel bedrijven dat internet gebruikt voor de ontvangst van orders duidelijk hoger (33%)[28].

Nederlandse bedrijven maken in 2008 ongeveer 12% van hun omzet via verkoop via internet[29]. In 1999 was maakte online verkoop nog maar 3% uit van de totale omzet. Wel is het aandeel van de omzet via internet in 2008 voor het eerst gedaald[30] (zie Figuur 4.3). De 12% omzet via internet ligt rond het gemiddelde van de 27 EU-landen. In Ierland (26%) en Noorwegen (21%) wordt een duidelijk groter deel van de omzet van bedrijven via internet gerealiseerd.

Wat betreft het aantal bedrijven dat het internet gebruikt als verkoopkanaal loopt Nederland dus voorop in Europa, maar wat betreft de omzet die via internet behaald wordt, behoort Nederland eerder tot de middenmoot[31].

Figuur 4.3 Ontwikkeling van de omzet van bedrijven via internet als % van de totale omzet, periode 1999–2008.



Bron: ICT-gebruik bedrijven, CBS, 2008.

ICT van groot belang voor bedrijven
Een belangrijk deel van het Nederlandse bedrijfsleven is voor haar bedrijfsprocessen sterk afhankelijk van ICT. Uit onderzoek van Ernst & Young uit begin 2010 blijkt dat 85% van de directeuren, managers en professionals vindt dat de bedrijfsprocessen binnen hun bedrijf in grote of zeer grote mate afhankelijk zijn van ICT (zie Figuur 4.4). Ruim één derde geeft aan dat de hun bedrijf volledig stil staat zonder ICT.

---

27 *Bron: De digitale economie 2009, CBS.*

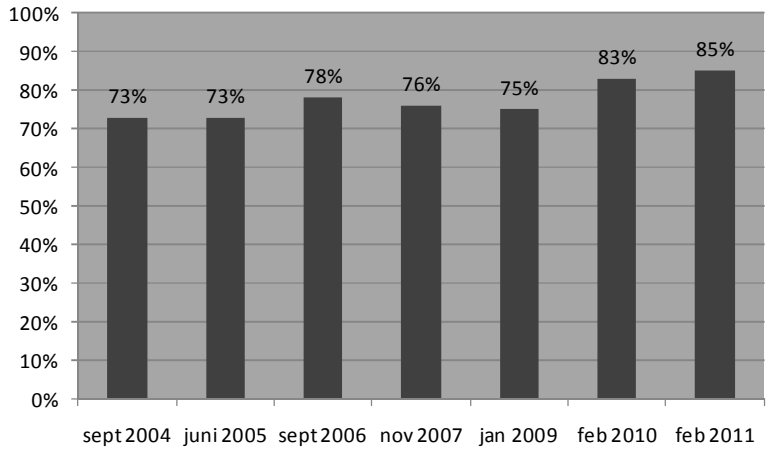
28 *Bron: Enterprises - Computers: Devices and communication systems (NACE Rev. 2), Eurostat, 09-09-2010.*

29 *Bron: ICT usage in enterprises 2009, Eurostat, Data in focus, 1/2010.*

30 *Bron: De digitale economie 2009, CBS. CBS geeft geen verklaring voor de daling van het omzetpercentage in 2008.*

31 *Op een belangrijke verklaring hiervoor gaan we in paragraaf 4.3.1 in. Het betreft het relatief lage bedrag dat Nederlandse consumenten besteden op internet (in vergelijking met andere Europese landen.*

Figuur 4.4 % directeuren, managers en professionals dat vindt dat de bedrijfsprocessen in hun bedrijf in (zeer) grote mate afhankelijk van zijn van ICT.



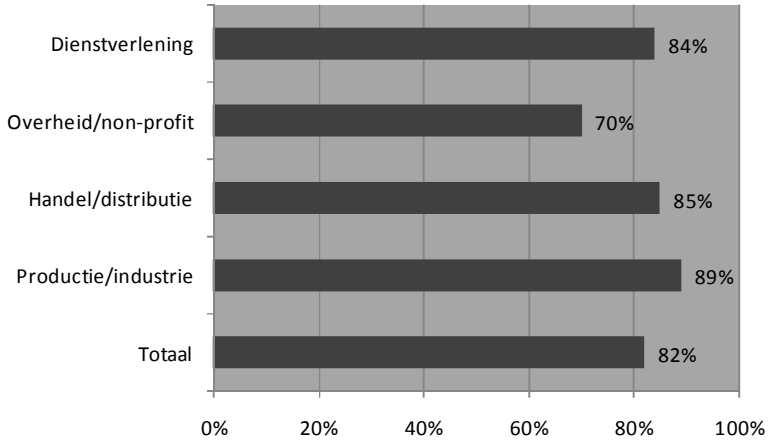
Bron: Cybercrime, ICT-barometer, Ernst & Young, februari 2011.

4.2.2 Vertrouwen in de ICT infrastructuur bij bedrijven

Bedrijven hebben veel vertrouwen in de eigen ICT veiligheid en betrouwbaarheid

Directeuren, managers en professionals hebben een hoge mate van vertrouwen in de ICT-veiligheid en –betrouwbaarheid binnen de eigen organisatie: 82% van de respondenten geeft begin 2011 aan veel vertrouwen te hebben in de beveiliging van de eigen organisatie tegen cybercrime. Bij productie/industriële bedrijven is het vertrouwen het hoogst (89%, zie Figuur 4.5).

Figuur 4.5 Vertrouwen in de beveiliging van organisaties tegen schade door cybercrime.



Bron: Cybercrime, ICT-barometer, Ernst & Young, februari 2011.

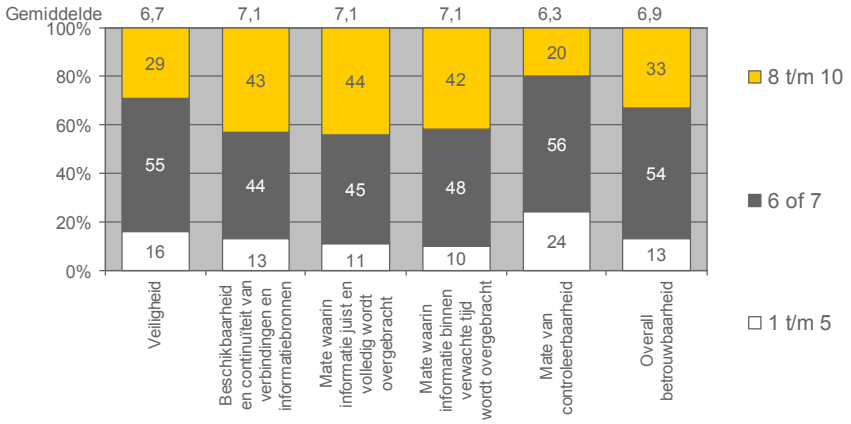
Het grote vertrouwen in de eigen beveiliging is opvallend, wanneer we de conclusies van hoofdstuk 3 in beschouwing nemen. Daar bleek dat relatief veel Nederlandse bedrijven worden getroffen door ICT veiligheidsincidenten. Ook bleek dat alleen al spam en netwerkuitval door oorzaken van buiten de organisatie het Nederlands bedrijfsleven naar schatting 1 tot 2 miljard euro kost op jaarbasis.

Voor het hoge vertrouwen in de eigen veiligheid worden door de bedrijven in de ICT-barometer verschillende redenen gegeven. De meest genoemde reden is dat zich binnen de eigen organisatie weinig of geen incidenten voordoen (62% van de bedrijven met veel vertrouwen). Ook heeft men het gevoel dat hun organisatie adequate beveiligingssystemen heeft (57% van de bedrijven met veel vertrouwen). Ongeveer één derde van de bedrijven met veel vertrouwen geeft aan dat er binnen de organisatie regelmatige aandacht voor cybercrime is (bewustwording), er adequate processen zijn om issues tijdig te detecteren en dat er binnen de organisatie een goede opvolging van incidenten is[32].

De veiligheid en betrouwbaarheid van de ICT-infrastructuur krijgt een zevenmin

In Figuur 4.6 is de waardering van de respondenten van de ICT-barometer weergegeven met betrekking tot de veiligheid en betrouwbaarheid van de Nederlandse ICT-infrastructuur. Uit de figuur blijkt dat directeuren managers en professionals uit het Nederlandse bedrijfsleven de veiligheid van de ICT-infrastructuur gemiddeld een 6,7 geven en de algehele betrouwbaarheid een 6,9.

Figuur 4.6 Waardering veiligheid en betrouwbaarheid Nederlandse ICT-infrastructuur



Bron: Veiligheid en betrouwbaarheid ICT-infrastructuur, ICT-barometer, Ernst & Young, september 2010.

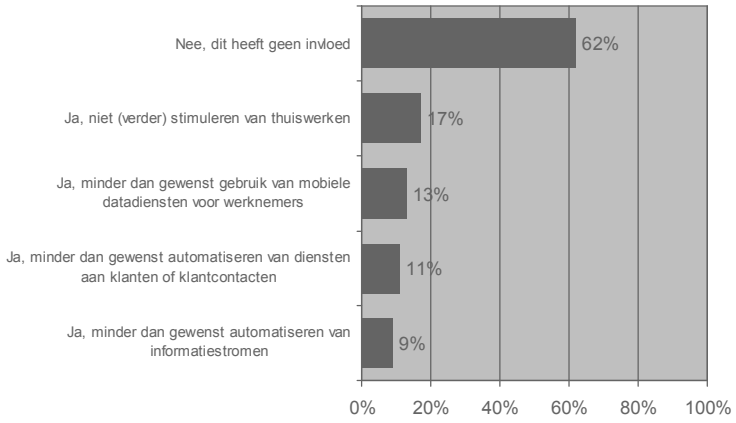
Als we kijken naar de kwaliteitsaspecten (voor uitleg zie paragraaf 2.4), dan valt op dat de controleerbaarheid van de Nederlandse ICT-infrastructuur met een 6,3 een stuk lager wordt gewaardeerd dan de andere kwaliteitsaspecten die ieder met een 7,1 worden gewaardeerd. Met controleerbaarheid wordt bijvoorbeeld bedoeld of te achterhalen is dat gegevens juist, volledig en tijdig zijn uitgewisseld. De lage waardering van de controleerbaarheid is opvallend. Immers, een vergelijking tussen de ontvangen en verzonden gegevens maakt het per definitie mogelijk om te analyseren of er verschillen juist en volledig zijn. Wellicht heeft de wat lagere waardering van de controleerbaarheid te maken met de complexiteit van het netwerk, waardoor het voor de eindgebruiker bij incidenten lastig te achterhalen waar of waarom er iets is fout gegaan.

32 *Het gaat hierbij om het beeld van de respondenten van het niveau van de veiligheidsprocessen van de organisatie, hetgeen niet per se overeen hoeft te komen met de feitelijke situatie.*

Vier op de tien bedrijven voelt zich door de veiligheid en betrouwbaarheid beperkt in de mogelijkheden

Figuur 4.7 laat zien dat 38% van de respondenten van de ICT-barometer het idee heeft dat de organisatie kansen voor verdere productiviteitsverbetering laat liggen als gevolg van onvoldoende vertrouwen in de veiligheid en betrouwbaarheid van de Nederlandse ICT infrastructuur[33]. In het onderzoek is daarbij specifiek gevraagd naar het faciliteren van de mogelijkheden om thuis te werken, het gebruik van mobiele datadiensten door werknemers, het automatiseren van diensten aan klanten en het automatiseren van informatiestromen.

Figuur 4.7 ICT-mogelijkheden waar uw organisatie geen of minder gebruik van maakt vanwege een te laag niveau van veiligheid en betrouwbaarheid van de Nederlandse infrastructuur.



Bron: Veiligheid en betrouwbaarheid ICT-infrastructuur, ICT-barometer, Ernst & Young, september 2010.

Respondenten bij grote bedrijven geven vaker aan dat hun bedrijf mogelijkheden niet gebruikt als gevolg van veiligheids- en betrouwbaarheidsredenen dan kleine, bijvoorbeeld als het gaat om gebruik van mobiele datadiensten door werknemers en het automatiseren van diensten aan klanten of klantcontacten.

Binnen de overheid/non-profit wordt met 28% het thuiswerken relatief vaak genoemd als mogelijkheid waar geen gebruik van wordt gemaakt vanwege veiligheids- en betrouwbaarheidsredenen. Dit kan te maken hebben met het feit dat overheidsorganisaties meer dan andere organisaties het voorkomen van onbevoegd gebruik van belang vinden. In de handel en distributie vormt het huidige niveau van veiligheid en betrouwbaarheid juist weinig beperking voor het verder stimuleren van thuiswerken.

4.2.3 Uitdagingen voor Nederland

Uit ons onderzoek komt naar voren dat ruim 80 % van de Nederlandse bedrijven een groot vertrouwen heeft in de ICT-beveiliging van de eigen organisatie. Tegelijkertijd geeft vier op de tien bedrijven aan zich als gevolg van veiligheidsissues beperkingen op te leggen in het gebruik van de technische mogelijkheden op het terrein van ICT.

---

33 *Het betreft hier de perceptie van de respondent. Ook andere overwegingen dan de veiligheid en betrouwbaarheid kunnen een rol spelen (bijvoorbeeld financiële overwegingen). Er is in het onderzoek niet gevraagd of deze overwegingen ook een rol spelen, noch naar het belang van deze verschillende afwegingen.*

Gevolg hiervan is dat veel bedrijven niet of niet volledig gebruik maken van de (technische) mogelijkheden om de dienstverlening aan de klant te digitaliseren en productiviteitsvoordelen te behalen.

Volgens de bedrijven zelf liggen er uitdagingen in de verbetering van de veiligheid en betrouwbaarheid van de ICT-infrastructuur *buiten* de eigen organisatie. Die uitdagingen liggen dan vooral bij de controleerbaarheid van datastromen. Dit kwaliteitsaspect krijgt van het bedrijfsleven het laagste rapportcijfer.

In contrast met de eigen inschatting dat de eigen beveiliging goed op orde is staat de constatering dat relatief veel Nederlandse bedrijven worden getroffen door ICT veiligheidsincidenten. In de interviews met brancheorganisaties wordt het beeld van het hoge vertrouwen van bedrijven in de eigen ICT-beveiliging bevestigd. Men geeft daarbij aan dat het eigen beveiligingsniveau door veel bedrijven wordt overschat.

Het genoemde contrast kent een tweetal invalshoeken:

- Een overschatting van de eigen beveiliging leidt tot kwetsbaarheden en meer veiligheidsincidenten. Dit tast uiteindelijk het vertrouwen aan. Dergelijke negatieve effecten hebben vaak een grotere impact dan positieve ervaringen.
- Een overschatting kan ook leiden tot het niet benutten van kansen tot productiviteitsverbetering. Dat is het geval wanneer men inschat dat de benodigde beveiliging om de productiviteitsverbetering te realiseren niet haalbaar is (technisch of qua kosten).

Een belangrijke uitdaging ligt dan ook in het bijstellen van de beeldvorming over het eigen beveiligingsniveau.

Een andere belangrijke uitdaging ligt volgens de geïnterviewden ook bij het besef dat bedrijven hebben in de eigen verantwoordelijkheid voor de veiligheid van de Nederlandse ICT infrastructuur. Met dit punt sluiten de geïnterviewde marktpartijen duidelijk aan bij een aantal conclusies eerder in dit hoofdstuk. De veiligheid van de infrastructuur wordt bepaald door het ingerichte stelsel van beveiligingsmaatregelen: op het niveau van serviceproviders, van de overheid en van dienstverleners (banken, internetwinkels, etc.), maar voor een belangrijk deel ook door de maatregelen die eindgebruikers (in dit geval bedrijven) zelf nemen om hun eigen informatiebronnen en netwerken te beveiligen. Eindgebruikers (bedrijven) hebben daarbij veel vertrouwen in de eigen beveiliging, terwijl zij toch relatief veel worden getroffen door incidenten.

4.3 Vertrouwen bij consumenten

4.3.1 Koopgedrag op internet van Nederlandse consumenten

Veel Nederlanders kopen en bankieren online

In het voorjaar van 2010 telde Nederland ruim 12 miljoen internetgebruikers[34]. Dat betekent dat 90% van de Nederlandse inwoners in de leeftijd van 12 tot 75 jaar in 2009 gebruik maakte van internet.

34 *Bron: Internetters bezorgd over online dreigingen, CBS, Persbericht 10-067, 26 oktober 2010.*

Ruim 80% van de volwassenen tussen de 16 en 74 jaar maakte in 2009 gebruik van internetbankieren. Hiermee staat Nederland in de top-3 van Europese landen. Met 87% van de volwassenen wordt in Estland en Finland nog intensiever gebruik gemaakt van internetbankieren[35]. Zweden en Denemarken volgen Nederland, met respectievelijk 79% en 77%, op de voet.

Als het gaat om het percentage volwassenen dat online producten en diensten aanschaft staat Nederland met 63% in Europa op een gedeelde derde plaats, samen met Zweden en scoort daarmee een stuk beter dan het Europees gemiddelde van 37%. Het Verenigd Koninkrijk en Denemarken scoren met respectievelijk 66% en 64% net iets hoger dan Nederland (zie Tabel 4.1).

Tabel 4.1 Mensen (leeftijd van 16 t/m 74) die, 12 maanden voorafgaand aan het onderzoek, producten of diensten voor privégebruik via het internet hebben aangekocht.

Land	2006	2007	2008	2009
Verenigd Koninkrijk	45%	53%	57%	66%
Denemarken	55%	56%	59%	64%
Zweden	55%	53%	53%	63%
Nederland	48%	55%	56%	63%
Duitsland	49%	52%	53%	56%
Finland	44%	48%	51%	54%
Frankrijk	22%	35%	40%	45%
België	19%	21%	21%	36%
Spanje	15%	18%	20%	23%
Polen	12%	16%	18%	23%
Italië	9%	10%	11%	12%
Noorwegen	-	-	-	-
EU-27 gemiddelde	**26%**	**30%**	**32%**	**37%**

Mensen (leeftijd van 16 t/m 74) die, 12 maanden voorafgaand aan het onderzoek, producten of diensten voor privégebruik via het internet hebben aangekocht

Bron: Internet usage in 2009 - Households and Individuals, Eurostat, Data in focus, 46/2009

Online verkopen sterk gestegen in de afgelopen 10 jaar

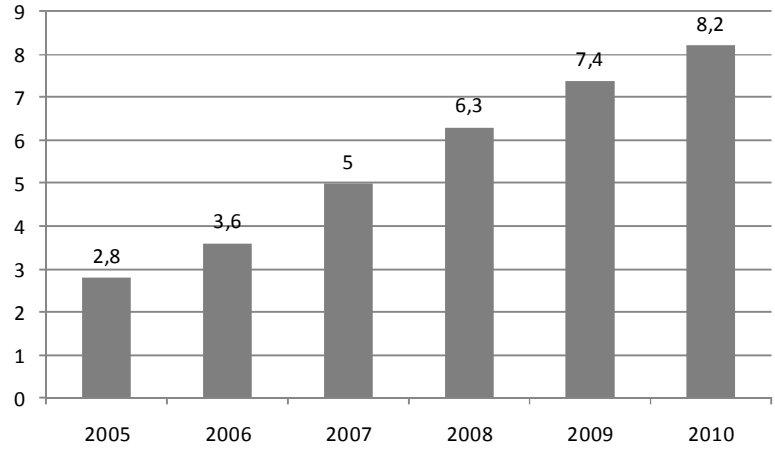
In 2010 werd in totaal 8,2 miljard euro uitgegeven door Nederlandse consumenten[36]. Daarmee maakte de totale online verkoop binnen Nederland iets meer dan 1% uit van het Bruto Nationaal Product[37]. In de afgelopen jaren zijn de online uitgaven van Nederlandse consumenten sterk gestegen(zie Figuur 4.8).

35 *Bron: E-Society, Office for National Statistics (UK), 2010.*

36 *Bron: Thuiswinkel Markt Monitor 2010-2, 2011.*

37 *Op basis van een BNP van 636 miljard euro (bron: CIA World Factbook).*

Figuur 4.8 Online consumentenbestedingen in de periode 1998 - 2010



Bron: Markt Monitor 2010-2, Thuiswinkel.org, 2011.

Jaarlijkse uitgaven online onder het Europees gemiddelde

Nederlandse consumenten gaven in 2010 888 euro uit online (zie Tabel 4.2)[38]. In 2009 was dat nog 857 euro. Dat is minder dan het Europees gemiddelde van 871 euro. In 2009 waren de absolute koplopers binnen Europa, als het gaat om de jaarlijkse uitgaven per consument via het internet, het Verenigd Koninkrijk (€1.240), Denemarken (€1.213) en Noorwegen (€1.102)[39].

Tabel 4.2 Online verkoop per consument per jaar, 2009.

Land	Online verkoop per consument per jaar	Aantal items aangeschaft
Verenigd Koninkrijk	€ 1.240	37
Denemarken	€ 1.213	24
Noorwegen	€ 1.102	13
Frankrijk	€ 995	20
Finland	€ 976	18
Italië	€ 935	17
Nederland[1]	€ 857	-
Zweden	€ 802	20
Spanje	€ 779	12
Duitsland	€ 765	22
Benelux	€ 709	16
Polen	€ 362	10
EU-27 gemiddelde	€ 871	20

[1]) Gegevens over Nederland afkomstig van Thuiswinkel.org

Bron: Kelkoo

Daardoor is het aandeel van de online verkoop als percentage van het BNP relatief laag

Door dit relatief lage online bestede bedrag per consument liggen de online verkopen in Nederland in termen van het aandeel van het totale bruto nationaal product lager dan in andere EU landen. In Nederland maken in 2009 de online bestedingen van consumenten ongeveer 1 procent uit van het Bruto Nationaal Product (zie tabel 4.3). In het Verenigd Koninkrijk en Denemarken ligt dit met 2% van het BNP en 1,9% duidelijk hoger.

38 *Bron: Markt Monitor 2010-2, Thuiswinkel.org, 2011.*

39 *Bron: European e-retail to buck the trend in 2010, Kelkoo press release, 2010.*

Door de geïnterviewden wordt aangegeven dat er voor deze beide koplopers qua online verkoop verschillende verklaringen zijn voor dit verschil in online bestedingen. Voor Denemarken wordt het verschil verklaard door een combinatie van 1) een vroege uitrol van een hoogwaardige ICT infrastructuur met hoge bandbreedtes en 2) een historisch gezien meer ontwikkelde thuiswinkel (postorder) cultuur. Als gevolg van de thuiswinkelcultuur waren consumenten al langer gewend aan kopen op afstand. Voor het Verenigd Koninkrijk ligt verklaring volgens de geïnterviewden in de grotere acceptatie van de creditcard als betaalmiddel.

Tabel 4.3 Online verkoop in verhouding met Bruto Nationaal Product, 2009.

Land	Online verkoop	BNP	Online verkoop als % van BNP
Verenigd Koninkrijk	€ 42,7 mrd.	€ 2154 mrd.	1,98%
Denemarken	€ 3,9 mrd.	€ 203 mrd.	1,92%
Finland	€ 2,6 mrd.	€ 184 mrd.	1,41%
Noorwegen	€ 3,3 mrd.	€ 253 mrd.	1,30%
Frankrijk	€ 24,7 mrd.	€ 2074 mrd.	1,19%
Duitsland	€ 33,4 mrd.	€ 2816 mrd.	1,19%
Nederland[1]	€ 7,4 mrd.	€ 636 mrd.	1,16%
Zweden	€ 3,8 mrd.	€ 337 mrd.	1,13%
Benelux	€ 8,3 mrd.	€ 1050 mrd.	0,79%
Spanje	€ 6,3 mrd.	€ 1337 mrd.	0,47%
Italië	€ 8,2 mrd.	€ 1814 mrd.	0,45%
Polen	€ 2,5 mrd.	€ 597 mrd.	0,42%

Bronnen: Kelkoo & CIA World Factbook

Nederlandse consument koopt vooral bij Nederlandse webwinkels
94% van de Nederlanders die online aankopen doen, doet dat bij Nederlandse webwinkels en 20% bij webwinkels uit andere EU-landen[40]. Landen als het Verenigd Koninkrijk en Duitsland vertonen hetzelfde gedrag.

4.3.2 Vertrouwen van de Nederlandse consument in de veiligheid van internet

Bijna driekwart van de Nederlandse internetgebruikers heeft in het afgelopen jaar te maken gehad met online veiligheidsproblemen
Bijna driekwart (72%) van de internetgebruikers in Nederland heeft in het afgelopen jaar te maken gehad met online veiligheidsproblemen (zie tabel 4.4). Tweederde van de internetgebruikers heeft te maken gehad met spam, ongeveer een kwart (24%) met virussen. Vijf procent van de Nederlandse internetgebruikers geeft aan in de afgelopen 12 maanden te maken te hebben gehad met misbruik van gegevens of schending van de privacy. Respectievelijk 2 en 1 procent zegt te maken te hebben gehad met phishing of fraude met betaalkaarten of creditcards[41]. Twee procent heeft te maken gehad met toegang van kinderen tot ongepaste websites of contact van kinderen met gevaarlijke personen (via internet.

40 *Bron: Internet usage in 2009 - Households and Individuals, Eurostat, Data in focus, 46/2009.*

41 *De Nederlandse Vereniging van Banken nuanceert deze uitkomst van het onderzoek van het CBS. In een persbericht van 27 oktober geven zij aan dat er in de eerste helft van 2010 514 phishing incidenten waren in Nederland.*

Tabel 4.4 Internetgebruikers die bezorgd zijn over en problemen hebben meegemaakt met online bedreigingen.

	% van alle internetgebruikers dat:	
	bezorgd is over	heeft meegemaakt
M.b.t. één of meerdere van onderstaande items	86%	72%
Virus of spam	65%	71%
Het krijgen van een computer virus	54%	24%
Het krijgen van ongewenste e-mails (spam)	48%	67%
Misbruik of financiële schade	77%	8%
Misbruik van persoonlijk gegevens of schending van privacy	67%	5%
Financiële schade door 'phishing'	50%	2%
Financiële schade door fraude met betaal- of creditkaarten	55%	1%
Kinderen toegang tot ongepaste websites of contact met gevaarlijke personen	41%	2%

Bron: Internetters bezorgd over online dreigingen, CBS, Persbericht 10-067, 2010.

Uit cijfers van Eurostat blijkt dan Nederlandse internetgebruikers in vergelijking met het Europees gemiddelde relatief vaak te maken hebben met spam, maar relatief weinig met virusinfecties. Het aantal internetgebruikers dat te maken heeft gehad met misbruik van persoonlijke gegevens of financiële schade ligt rond het Europees gemiddelde[42].

Een ruime meerderheid van de Nederlandse internetgebruikers is bezorgd over online dreigingen

Uit onderzoek van het CBS blijkt dat een ruime meerderheid van de Nederlandse internetgebruikers (2009: 86%) zich zorgen maakt over dreigingen vanaf het internet. Ongeveer driekwart van de internetgebruikers maakt zich zorgen over misbruik of financiële schade. Ruim de helft (65%) van de internetgebruikers is bezorgd over problemen met virussen en spam (zie Tabel 4.4).

Interessant is ook de vergelijking tussen bezorgdheid en eigen ervaring. Uit tabel 4.4 komt naar voren dat de bezorgdheid over misbruik van gegevens, financiële schade door phishing of fraude met betaalkaarten in vrijwel alle gevallen niet gebaseerd is op eigen ervaringen (in hetzelfde jaar).

Ten minste één miljoen Nederlanders koopt niet online vanwege vertrouwensaspecten

De bezorgdheid over online dreigingen vormt voor een deel van de Nederlandse internetgebruikers een belemmering om online aankopen te doen. In 2009 deden 3 miljoen internetgebruikers in Nederland geen online aankopen (ongeveer één kwart). Een belangrijk deel van hen deed dit (onder andere) niet vanwege een gebrek aan vertrouwen in de veiligheid van internettransacties (35%), in de privacy (27%) en/of in de levering van de bestelde goederen en diensten (23%) (zie tabel 4.5). In totaal schatten wij op basis van deze cijfers in dat ten minste 1 miljoen Nederlanders geen goederen of diensten op internet koopt vanwege vertrouwensaspecten. Overigens is het waarschijnlijk dat (een gebrek aan) vertrouwen in de veiligheid van internettransacties, in de privacy en in de levering ook voor een deel van de consumenten die wel online aankopen doen een reden is om minder online aankopen te doen.

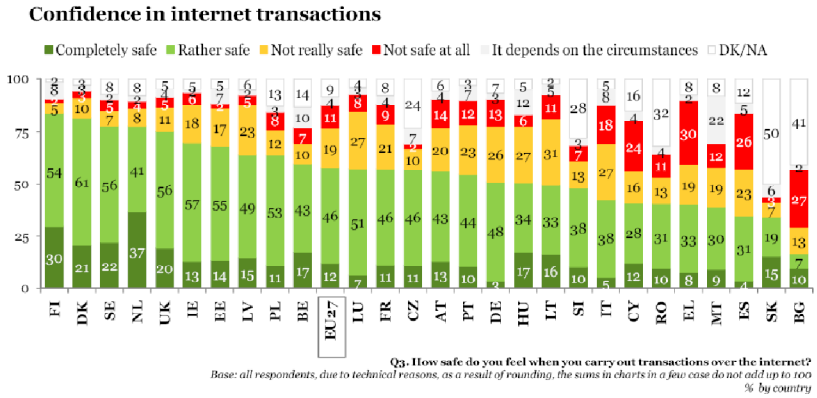
42 *Bron: Eurostat, 2010.*

Internationale vergelijking

Een belangrijk deel van de Nederlandse internetgebruikers is dus bezorgd over internetdreigingen en een niet onaanzienlijk deel van de internetgebruikers doet geen online aankopen (onder andere) vanwege vertrouwensaspecten. Wijken we daarmee af van andere landen in Europa?

Uit de statistieken van Eurostat blijkt dat Nederland wat betreft het vertrouwen van consumenten in online-transacties in de top van Europa meedraait. Bijna 80 procent van de Nederlandse internetgebruikers gaf in 2008 aan internettransacties enigszins of volkomen veilig te vinden. Dat is vergelijkbaar met het niveau in de Scandinavische landen en het Verenigd Koninkrijk (zie Figuur4.9). Eerder constateerden we dat in onder andere Denemarken en het Verenigd Koninkrijk duidelijk meer online wordt uitgegeven dan in Nederland. Het vertrouwen in internettransacties lijkt hier geen bepalende factor bij te zijn.

Figuur 4.9 Vertrouwen van internetgebruikers in transacties via het internet.



Bron: Confidence in the Information Society Analytical Report, EC, Flash Eurobarometer 250, May 2009.

Kijken we naar de consumenten die (nog) geen online aankopen doen (in Nederland 3 miljoen consumenten), dan zien we dat er hier wel een verschil te zien is. In vergelijking met landen als Ierland, Noorwegen, Denemarken en het Verenigd Koninkrijk speelt in Nederland onvoldoende vertrouwen in de veiligheid van betalingstransacties, in privacyaspecten en in de levering een duidelijk belangrijkere rol bij de keuze om geen online-aankopen te doen (zie Tabel 4.5).

Tabel 4.5 Percentage van mensen die geen goederen of diensten via internet kopen vanwege vertrouwensaspecten.

Land	Veiligheid betalingstransactie	Privacyaspecten	Vertrouwen in de levering
Polen	5%	7%	9%
Ierland	10%	6%	3%
Italië	20%	11%	15%
Noorwegen	23%	18%	12%
Denemarken	25%	21%	8%
Verenigd Koninkrijk	27%	18%	8%
België	35%	20%	18%
Nederland	***35%***	***27%***	***23%***
Duitsland	37%	31%	27%
Zweden	50%	48%	30%
Finland	59%	59%	37%
Frankrijk	69%	50%	52%
Europese Unie (27 landen)	**35%**	**29%**	**26%**

Bron: Perceived barriers to buying/ordering over the Internet, Eurostat, Dataset ISOC_EC_INB, 2009

4.3.3 De economische potentie van meer vertrouwen in de veiligheid van internet

Er zijn weinig onderzoeken naar de relatie tussen de economie en het vertrouwen in de digitale economie. Een omvattend onderzoek naar dit onderwerp op Europees niveau betreft een onderzoek uitgevoerd door Booz & Co[43]. In dit onderzoek worden drie scenario's uitgewerkt. In het basis scenario wordt er van uitgegaan dat er geen grote veranderingen optreden in hoe de sector de veiligheidsproblemen aanpakt. In het best case scenario wordt gekozen voor een geharmoniseerde aanpak van digitaal vertrouwen vanuit een gezamenlijke visie. In het worst case scenario gaan alle spelers hun eigen weg, zij opereren onafhankelijk van elkaar zonder gemeenschappelijke visie.

In haar analyse komt Booz & Co tot de conclusie dat de risico's (het worst case scenario wordt realiteit) in economische termen groter zijn dan de voordelen van het best case scenario. Concreet schat Booz & Co in dat in het worst case scenario het inkomsten volume van de Europese digitale economie 18% lager kan uitvallen dan in het basisscenario. In het best case scenario schat Booz & Co in dat de inkomsten van de digitale economie 11% hoger kunnen uitvallen. Voor alleen het onderdeel e-commerce komt Booz & Co uit op een potentieel voordeel van 10% van de geschatte Europese e-commerce inkomsten en een potentieel risico van 20%.

Vertaling naar Nederland

Hieronder vertalen wij de scenario's van Booz & Co door naar de Nederlandse situatie. Booz & Co biedt in haar rapport weinig inzicht in de veronderstellingen die ten grondslag hebben gelegen aan inschatting van de extra potentie en het risico. Een meer geavanceerde vertaling van de resultaten van het onderzoek naar de Nederlandse situatie is daardoor niet goed mogelijk. Wij kiezen daarom voor een één-op-één doorvertaling zonder daar op bewerkingen los te laten. Deze één-op-één doorvertaling biedt een grof inzicht in de orde van grootte van de economische potentie en het economische risico wanneer wel of juist niet extra wordt geïnvesteerd in meer vertrouwen in de ICT bij de eindgebruiker.

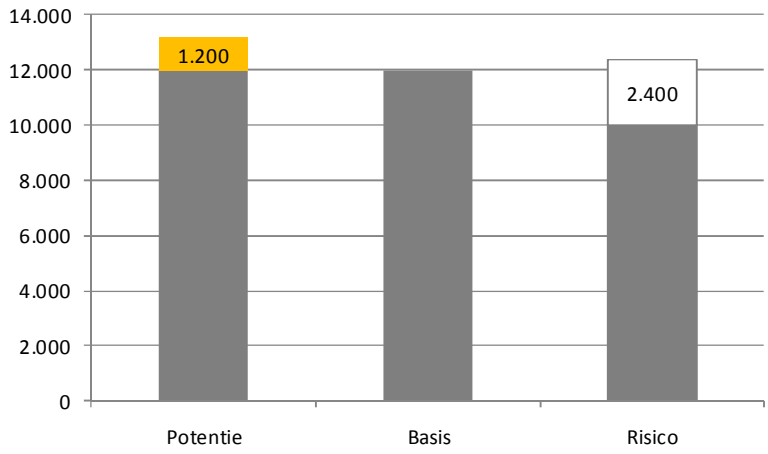
43 *Digital confidence, Booz & Company, 2008.*

De analyse van Booz & Co gaat uit van 2008 als basisjaar en schat vervolgens de potentie en het risico van meer vertrouwen in de ICT-veiligheid bij de consument in richting 2012. In de doorvertaling is 2011 als basis genomen en worden de door Booz & Co ingeschatte potentie en risico's geprojecteerd op 2014. Wij richten ons daar alleen op het belangrijkste deel van de digitale economie: e-commerce. Voor het basisscenario is uitgegaan van een groei van de internetverkopen van 10% jaarlijks, hetgeen overeenkomt met internationale voorspellingen over de ontwikkeling van de online retailmarkt in Nederland.

De doorvertaling van de scenario's naar de Nederlandse situatie levert het volgende beeld op:

- in het basisscenario kopen Nederlandse consumenten in 2014 voor 12 miljard euro goederen en diensten online;
- het best case scenario van Booz & Co biedt in de Nederlandse verhoudingen een extra potentie in de orde van grootte van maximaal 1,2 miljard euro;
- het worst case scenario betekent in Nederlandse termen een potentieel risico in de orde van grootte van 2,4 miljard euro.

Figuur 4.10 Vertaling schatting Booz & Co potentie en risico investeren in digital confidence op de omvang van internetverkopen naar de Nederlandse situatie in 2014 (in miljoenen euro's)



Bron: Schatting E&Y op basis van bron: 'Digital confidence', Booz & Co, 2008.

De extra groei in internetverkopen kan voortkomen uit een toename in aankopen van consumenten die ook op dit moment gebruik maken van de mogelijkheden van e-commerce. Gezien het eerder in dit hoofdstuk geconstateerde verschil in het gemiddelde bestede bedrag per onlineconsument in Nederland, in vergelijking met bijvoorbeeld Denemarken en het Verenigd Koninkrijk, ligt hier nog potentie. Een aantal geïnterviewden geeft aan dat er bij het verschil in de omvang van internetaankopen weliswaar geen directe relatie lijkt te liggen met vertrouwensaspecten (historisch zijn er andere oorzaken), maar dat het investeren in meer vertrouwen wel degelijk een belangrijke bijdrage kan leveren in het vergroten van het bestede bedrag op internet.

Een andere belangrijke potentie ligt bij de groep consumenten die op dit moment nog geen online aankopen doet, omdat zij bezorgd is over de veiligheid van online betalingstransacties, over privacyaspecten of over de levering.

Wanneer de één miljoen internetgebruikers die nu nog geen online aankopen vanwege vertrouwensaspecten wel online aankopen zouden doen en daarbij hetzelfde koopgedrag vertonen als de consumenten die wel online aankopen doen dan zou dit voor de digitale economie in Nederland extra inkomsten met een equivalent van jaarlijks ongeveer 900 miljoen euro betekenen (1 miljoen maal 888 euro per consument)[44].

Een extra economische potentie in de orde van grootte van 1 miljard euro bij een toename van het vertrouwen achten wij gezien het bovenstaande in als realistisch aangezien ook de aankopen van bestaande kopers naar verwachting zullen toenemen.

Over de omvang van de potentiële economische schade als gevolg van een minder groot vertrouwen in ICT hebben wij geen data kunnen vinden. Dat maakt het inschatten van de plausibiliteit het economische risico van een afname van het vertrouwen in internet voor Nederland lastig.

Overigens gaat het bij de inschatting van het potentieel en de potentiële inschatting van het risico om een bruto inschatting. Voor een deel zal het gaan om substitutie van aankopen uit de fysieke handel naar online-aankopen. Voorbeelden hiervan zijn zichtbaar in de reisbranche, waarin een groot deel van de boekingen inmiddels online plaatsvindt en bijvoorbeeld op het terrein van multimedia (muziek, film, games) waar een steeds groter deel van de aankopen online (en digitaal) plaatsvindt. Uit onderzoek blijkt echter ook dat er sprake is van complementariteit. Onderzoek van het Ruimtelijk Planbureau uit 2007 laat zien dat voor 14 procent[45] van de internetaankopen (exclusief de tweedehandsmarkt) geldt dat het gaat om extra aankopen die zonder het internet niet zouden hebben plaats gevonden[46].

Naast extra aankopen biedt e-commerce vooral een aantal efficiencyvoordelen. Het lagere kostenniveau van internetwinkels leidt bijvoorbeeld tot efficiencyvoordelen en lagere prijzen voor de consument. Bij dit laatste speelt ook de grotere transparantie van de markt een rol. E-commerce heeft bijvoorbeeld geleid tot prijsbewuster aankoopgedrag bij consumenten, doordat eenvoudiger een vergelijking kan worden gemaakt tussen aanbieders[47]. Ook voor de winkelier met een fysieke winkellocatie zijn er overigens efficiencyvoordelen mogelijk. De consument oriënteert zich bijvoorbeeld op internet en kan daardoor in de fysieke winkel efficiënter worden geholpen.

---

44 *Het gaat hierbij zowel om extra consumptie als om verschuiving van aankopen in de fysieke economie naar de digitale economie.*

45 *Het betreft cijfers over 2007. Gezien de ontwikkelingen van de onlinemarkt in de afgelopen jaren en de verwachte ontwikkelingen in de periode tot 2014 is het waarschijnlijk dat deze verhouding op dat moment duidelijk anders is.*

46 *Ruimtelijk Planbureau, Winkelen in het internettijdperk, 2007.*

47 *Weltevreden, J.W.J., City centres in the Internet age. Exploring the implications of b2c e-commerce for retailing at city centres in the Netherlands, 2006 en Weltevreden, J.W.J., 'Substitution or complementarity? How the Internet changes citycentre shopping', Journal of Retailing and Consumer Services, 2007.*

4.3.4 Uitdagingen voor Nederland

In paragraaf 4.3.3 is een inschatting gegeven van de economische potentie (orde van grootte van 1,2 miljard euro in 2014) die een verdere vergroting van het vertrouwen van consumenten in de veiligheid en betrouwbaarheid van internet biedt in termen van meer online aankopen van consumenten. De belangrijkste uitdaging ligt er in om deze economische potentie te realiseren.

Daarvoor is het van belang om te blijven investeren in maatregelen die ook nu al veel aandacht krijgen, zoals:

- de aanpak van cybercrime;
- voorlichting over de werkelijke risico's en voordelen van internetgebruik en online-winkelen en –bankieren;
- versterken van de bewustwording van de eigen verantwoordelijkheid van consumenten in het vergroten van de eigen veiligheid op internet (digibewust).

Een van de opvallende conclusies van paragraaf 4.3 is dat consumenten zich relatief veel zorgen maken over misbruik van persoonlijke gegevens, schending van privacy en financiële schade door phishing of fraude met betaalmiddelen, terwijl maar een zeer klein deel van de consumenten daar zelf door getroffen wordt.

Ook bleek in paragraaf 4.3 dat voor ruim één miljoen consumenten een gebrek aan vertrouwen in de veiligheid van internettransacties, in de privacy en/of in de levering van de bestelde goederen en diensten een belangrijke reden is om geen online aankopen te doen.

Een belangrijke uitdaging ligt er dan ook in om consumenten meer vertrouwen te geven dat er goed met hun gegevens wordt omgegaan, dat betalen via internet veilig is en dat de goederen en diensten die zij aankopen ook geleverd worden.

Uiteindelijk gaat het er overigens om de netto-meerwaarde van online winkelen te vergroten. Wanneer er immers alleen sprake is van een substitutie van het fysieke naar het online kanaal zonder doelmatigheidsvoordelen dan levert deze substitutie de Nederlandse economie geen voordelen op.

In hoofdstuk 6 gaan we dieper in op de aanbevelingen die volgen uit deze uitdagingen.

4.4 Conclusie

Het vertrouwen van consumenten en bedrijven in de veiligheid en betrouwbaarheid van de Nederlandse ICT infrastructuur is een bepalende factor in het gebruik dat zij maken van die infrastructuur. Bij vertrouwen gaat het daar bij om verschillende aspecten, zoals het vertrouwen dat er geen misbruik wordt gemaakt van persoonlijke gegevens en dat de privacy niet geschonden wordt, vertrouwen dat financiële transacties op een veilige manier plaatsvinden en vertrouwen dat goederen en diensten die online worden besteld ook geleverd worden. Ook het vertrouwen in de beschikbaarheid is van belang.

Hieronder geven we de belangrijkste conclusies van dit hoofdstuk weer. De hoofdvragen die daarbij centraal staan zijn:

- Hoe is het gesteld met het vertrouwen van Nederlandse bedrijven en consumenten in de Nederlandse ICT infrastructuur?
- Welke (economische) meerwaarde kan een versterking van het vertrouwen bij bedrijven en consumenten opleveren?
- Waar liggen mogelijkheden om het vertrouwen te vergroten?

Vertrouwen bij het bedrijfsleven

- Uit ons onderzoek komt naar voren dat Nederlandse bedrijven vertrouwen hebben in de veiligheid en betrouwbaarheid van de Nederlandse ICT infrastructuur. De veiligheid van de Nederlandse ICT infrastructuur krijgt van het Nederlandse bedrijfsleven het rapportcijfer 6,7. De betrouwbaarheid scoort een 6,9. Een ruime voldoende, maar er is ruimte voor verdere verbetering. Die ruimte is er op alle veiligheids- en betrouwbaarheidsattributen, maar in het bijzonder bij het vertrouwen in de controleerbaarheid van de datastromen over de ICT infrastructuur. Dit wordt het laagst beoordeeld. Ook het adresseren van zorgen bij bedrijven rond de veiligheid van bedrijfsgegevens in externe informatiesystemen kan bijdragen aan een groter vertrouwen bij bedrijven in de veiligheid en betrouwbaarheid van de ICT infrastructuur.
- Het vertrouwen in de beveiliging van de eigen organisatie tegen aanvallen van buitenaf is hoog. 80 procent van de bedrijven uit de ICT barometer heeft veel vertrouwen in de eigen beveiliging tegen cybercrime.
- Ondanks de het grote vertrouwen in de eigen ICT beveiliging geeft 4 op de 10 bedrijven in ons onderzoek aan de technische mogelijkheden van de ICT infrastructuur niet volledig te benutten vanwege veiligheidsaspecten. Daarmee laten de bedrijven in potentie belangrijke productiviteitsvoordelen liggen. Zo maken Nederlandse bedrijven voor hun verkopen nog relatief weinig gebruik van internet.
- Het aandeel van de omzet die Nederlandse bedrijven generen via het internet (ruim 10 procent van het totaal) ligt weliswaar rond het Europees gemiddelde. In landen die tot de top van Europa behoren op dit gebied wordt echter 20-25 procent van de omzet gegenereerd via internet (Ierland en Noorwegen).
- Het hoge vertrouwen in de eigen ICT beveiliging vormt in potentie een belangrijke belemmering om verdere productiviteitsvoordelen te realiseren. Dat is het geval wanneer men (onterecht) inschat dat verdere beveiligingsmaatregelen niet meer mogelijk zijn of een zeer hoge investering vereist. Een belangrijke uitdaging ligt dus mogelijk in een realistische beeldvorming van het beveiligingsniveau van de eigen organisatie van bedrijven en van de voordelen van het investeren in de kansen die ICT nog biedt en de daarbij behorende kosten, waaronder beveiligingskosten.
- Een andere belangrijke uitdaging die uit het onderzoek naar voren komt, ligt bij het stimuleren van het besef bij bedrijven van de eigen verantwoordelijkheid voor de veiligheid van de Nederlandse ICT infrastructuur. Ook hierbij gaat het allereerst om het creëren van een realistisch beeld van de eigen beveiliging en de mogelijkheden om die te verbeteren. Op korte termijn betekent dit mogelijk een lager vertrouwen in de ICT veiligheid. Op langere termijn zal het realistische beeld en het besef van eigenverantwoordelijkheid daarentegen moeten leiden tot een hoger gemiddeld ICT-veiligheidsniveau en een hoger vertrouwen.

Vertrouwen bij de consument

- Meer vertrouwen in de veiligheid en betrouwbaarheid van internet bij consumenten heeft economische potentie. Op basis van een doorvertaling van een Europese studie van Booz & Co naar de Nederlandse verhoudingen schatten we in dat een hoger vertrouwen bij consumenten in 2014 een (bruto-)potentie heeft in de orde van grootte van 1,2 miljard euro aan extra online e-commerce omzet.
- Deze potentie is te realiseren door het vergroten van de groep consumenten die online aankopen doet en door het verhogen van het bestede bedrag per consument. Bij beide groepen ligt vanuit het vertrouwen het perspectief van vertrouwen in de veiligheid van internet potentie.
- Minimaal 1 miljoen internetgebruikers in Nederland doen op dit moment nog geen aankopen op internet vanwege gebrek aan vertrouwen in de veiligheid van internet In vergelijking met landen als het Verenigd Koninkrijk en Denemarken hebben relatief veel Nederlandse consumenten die niet online kopen veiligheidbezwaren. Zouden de genoemde 1 miljoen internetgebruikers wel online aankopen doen, dan zou de online omzet in potentie jaarlijks 900 miljoen euro hoger kunnen liggen.
- Voor de groep Nederlandse consumenten die al wel online aankopen doet geldt dat het bedrag dat zij jaarlijks online uitgeven relatief laag is (zie tabel 4.6). In Nederland hebben de onlineverkopen een waarde van ongeveer 1 procent van het BNP. In het Verenigd Koninkrijk en Denemarken is dat twee maal zo hoog (2% van het BNP).

Tabel 4.6 Benchmark Europese landen op het terrein van 'online verkoop' (2009).

	Percentage online consumenten	Online verkoop per consument (in €)	Online verkoop (in mld. €)	Online verkoop als % BNP
Verenigd Koninkrijk	66%	1239,51	42,7	1,98%
Denemarken	64%	1213,25	3,9	1,92%
Finland	54%	975,56	2,6	1,41%
Noorwegen	-	1101,69	3,3	1,30%
Frankrijk	45%	994,65	24,7	1,19%
Duitsland	56%	764,98	33,4	1,19%
Nederland	***63%***	***857,00***	***7,4***	***1,16%***
Zweden	63%	801,79	3,8	1,13%
Spanje	23%	778,65	6,3	0,47%
Italië	12%	934,67	8,2	0,45%

Bron: Eurostat, Kelkoo, CIA World Factbook, Thuiswinkel.org

- Uit ons onderzoek komt naar voren dat er geen direct verband lijkt te zijn tussen de lagere besteding van Nederlanders op internet en verschillen in vertrouwen in de veiligheid van internet. Wel biedt het versterken van het vertrouwen mogelijkheden om de verschillen met landen als Denemarken en het Verenigd Koninkrijk te verkleinen. Deze mogelijkheden liggen naast de reeds bestaande maatregelen, zoals onder andere het programma Digibewust en de aanpak van feitelijke veiligheidsincidenten vooral in de versterking van het vertrouwen van consumenten in de veiligheid van betalingsmethoden en de veilige omgang met en opslag van hun gegevens door aanbieders op internet. Consumenten zijn bezorgd over deze aspecten. Deze bezorgdheid in gebaseerd op de perceptie van de kans op misbruik van persoonlijke gegevens die zij lopen

en de bezorgdheid over de gevolgen wanneer dat gebeurt (bijvoorbeeld bij phishing en fraude met betaalkaarten).

- Uiteindelijk gaat het er om de netto-meerwaarde van online winkelen te vergroten. Wanneer er immers alleen sprake is van een substitutie van het fysieke naar het online kanaal zonder doelmatigheidsvoordelen dan levert deze substitutie de Nederlandse economie geen voordelen op.

5 Het belang voor het vestigingsklimaat

5.1 Inleiding

In dit hoofdstuk richten wij ons op het belang van (veilige en betrouwbare) ICT-infrastructuur als vestigingsplaatsfactor. ICT is van groot belang voor bedrijven in de software sector of voor data centra, maar ook voor bedrijven in bijvoorbeeld de financiële- en zakelijke dienstverlening en de logistiek speelt ICT een belangrijke rol in de dagelijkse werkzaamheden. In dit hoofdstuk proberen wij een antwoord te vinden op de volgende vragen:

- Hoe scoort Nederland wat betreft kwaliteit en de veiligheid en betrouwbaarheid van de ICT-infrastructuur ten opzichte van andere landen?
- Hoe belangrijk is de veiligheid en betrouwbaarheid van de ICT-infrastructuur als vestigingsplaatsfactor?

5.2 Het Nederlandse vestigingsklimaat

Het begrip investeringsklimaat (ook wel vestigingsklimaat) duidt op een totaalsom van factoren op basis waarvan de aantrekkelijkheid voor investeringen wordt afgemeten. Dit betekent dat het een containerbegrip is, waarvan de inhoud kan verschillen. Hieronder vallen onder meer politieke instabiliteit, de machtsverhouding tussen het politieke centrum en haar regio's, corruptie, het belastingsysteem en de wet- en regelgeving. Het investeringsklimaat van landen is afhankelijk van allerlei factoren en kan daardoor sterk verschillen[48].

Zodra buitenlandse bedrijven investeren in Nederland, bijvoorbeeld in de vorm van een hoofdkantoor, een laboratorium of een distributiecentrum, levert dit naast kapitaalinstroom en belastinginkomsten een verbeterde reputatie en een vergrote kans op zakenrelaties met het Nederlandse bedrijfsleven op. Zo hebben zich op de Amsterdamse Zuidas relatief veel buitenlandse bedrijven gevestigd, wat zichtbaar bijdraagt aan de kracht en potentie van dit gebied. Indirect lijken de effecten nog groter: met name hoofdkantoren hebben een richtinggevende werking op de economie. Alleen al de gedachte dat bijvoorbeeld Shell, ING en Philips zouden overwegen hun hoofdkantoor te verplaatsen naar buiten Nederland zou het vertrouwen in de Nederlandse economie schaden.

Locatiebeslissingen in het begin van de 21e eeuw zijn als volgt te kenmerken:

1 Ondanks kleiner wordende afstanden (door onder meer betere ICT en bereikbaarheid) is er nog geen sprake van death of distance: locatie doet er toe en steden herleven als centra met kennis en netwerken.
2 De strijd om arbeidstalent onderstreept het belang van toegankelijke locaties en een aantrekkelijke werk- en woonomgeving.

48 *Bron: De externe factor? Westerse olie- en gasbedrijven en het Russische investeringsklimaat 1992-2000, d'Arnaud Gerkens, 2006.*

3 Steden spelen een essentiële rol bij het aantrekken van investeringen in een regio.
4 Terwijl vaardigheden van personeel belangrijker worden neemt het belang van flexibiliteit toe als sleutelkenmerk van een locatie. Hierbij gaat het zowel om geografische flexibiliteit als om het aanpassingsvermogen van werknemers aan een nieuwe functie (de employability van het personeel).
5 De vestiging van faciliteiten, met name van (Europese) hoofdkantoren, volgt in 40% van de gevallen eerdere investeringen. Vaak betreft dit marketing & sales en (soms) onderwijs&training, logistiek, Shared Service centers, productie en / of R & D.

Aantrekkelijkheid van Nederland
Ruim 3.000 bedrijven vestigen zich jaarlijks buiten hun landsgrenzen in Europa. Nederland neemt daarvan ruim 3% voor haar rekening, een redelijk stabiel deel. In de top 20 van de meest aantrekkelijke Europese investeringslanden stijgt Nederland van de tiende positie in 2008 naar de zevende in 2009. Daarbij gaat het vooral om vestigingen van sales & marketingkantoren en logistieke centra. Belangrijke sectoren zijn de zakelijke dienstverlening, software en logistiek.

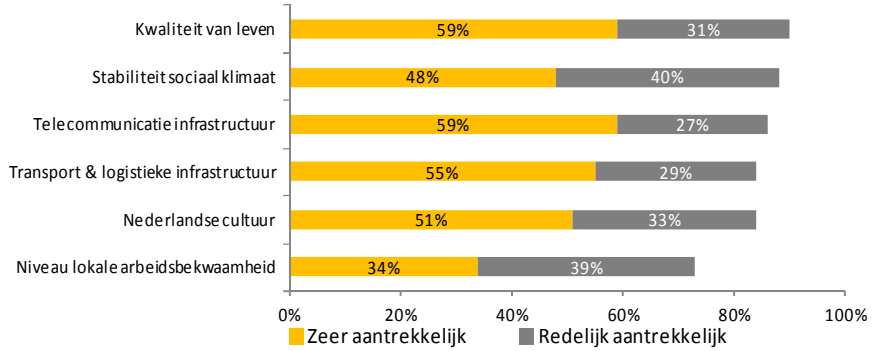
De cijfers maken duidelijk dat Nederland nog altijd een aantrekkelijke vestigingsplaats is voor buitenlandse bedrijvigheid. Dat heeft te maken met de geografische ligging van ons land als 'Gateway to Europe' naast andere factoren zoals de kwaliteit van wonen en werken en een stabiel sociaal klimaat. Ook onze infrastructuur en de aanwezigheid van belangrijke mainports als de luchthaven Schiphol en de haven van Rotterdam zijn factoren die meewegen in de locatiekeuze van een buitenlandse onderneming. Ten slotte is het Nederlandse belastingklimaat een belangrijk voordeel voor vestiging in Nederland.

5.3 Aantrekkelijkheid van de Nederlandse ICT infrastructuur

ICT infrastructuur een sterk punt van het Nederlandse vestigingsklimaat
In de Barometer Nederlands vestigingsklimaat (2010)[49] van Ernst & Young wordt telecommunicatie infrastructuur als nummer drie genoemd van de sterke punten van het Nederlands vestigingsklimaat. Het volgt na de kwaliteit van leven en de stabiliteit van het sociale klimaat van Nederland (zie Figuur 5.1). 86% van de respondenten vindt de telecommunicatie infrastructuur een aantrekkelijke factor van Nederland.

49 *Bron: Ernst & Young, Barometer Nederlands Vestigingsklimaat 2010, Open vizier voor nieuwe kansen*

Figuur 5.1 Sterke punten ten aanzien van het Nederlands vestigingsklimaat 2010 (203 respondenten).

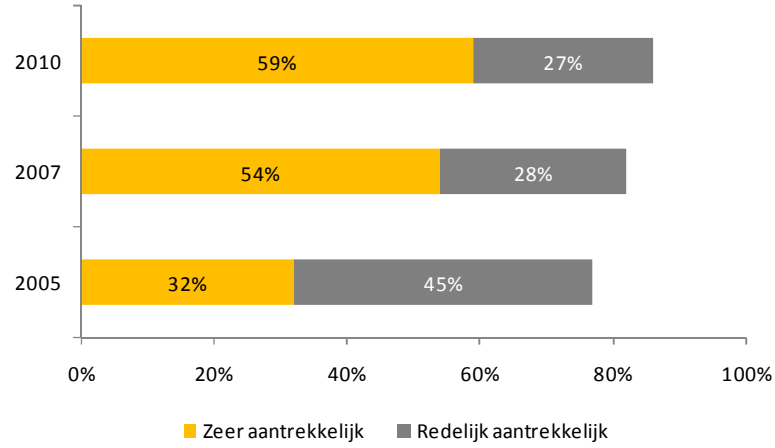


Bron: Barometer Nederlands Vestigingsklimaat, Open vizier voor nieuwe kansen, Ernst & Young, 2010.

Telecominfrastructuur als steeds aantrekkelijker beoordeeld

Uit onderzoek van Ernst & Young[50] blijkt dat Nederland door de jaren heen steeds beter is gaan scoren op het gebied van de telecommunicatie infrastructuur. De score van Nederland op het terrein van telecom als locatiefactor is door de jaren heen verbeterd. In 2005 vond 77% van de respondenten telecommunicatie infrastructuur een sterk punt van het Nederlands vestigingsklimaat, in 2007 groeide dit percentage naar 82% en in 2010 vond 86% van de respondenten de telecommunicatie infrastructuur van Nederland aantrekkelijk.

Figuur 5.2 % buitenlandse bedrijven dat de telecominfrastructuur als een aantrekkelijk punt van het Nederlandse vestigingsklimaat beoordeelt (2005, 2007 en 2010)



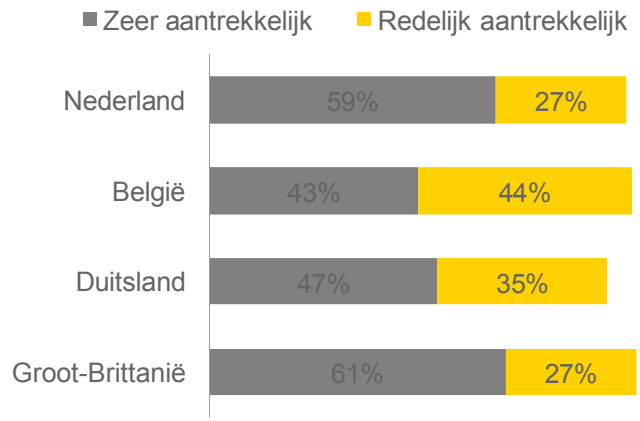
Bron: Netherlands attractiveness survey, Ernst & Young, 2010, 2007 en 2005

Ook omliggende landen hebben een aantrekkelijke telecominfrastructuur

Uit Ernst & Young studies naar het vestigingsklimaat in Nederland, België, Duitsland en het Verenigd Koninkrijk komt het beeld naar voren dat deze landen een telecominfrastructuur kennen die qua aantrekkingskracht wedijvert met die van Nederland. Het aandeel bedrijven dat de telecominfrastructuur als aantrekkelijk beschouwd wisselt niet sterk tussen Nederland, België, Duitsland en het Verenigd Koninkrijk (zie Figuur 5.3).

50 *Bron: Barometer Nederlands Vestigingsklimaat 2010, 2007 en 2005*

Figuur 5.3 Aantrekkelijkheid telecommunicatie infrastructuur in Nederland en omliggende landen.



Bron: Ernst & Young, 2010.

Nederland wereldwijd in de top 5 van landen met een kwalitatief goede ICT infrastructuur

In onderzoek van IBM en The Economist Intelligence uit 2010 naar de kwaliteit van de ICT-infrastructuur van landen[51] scoort Nederland een 5e plaats wereldwijd. In een vergelijkbaar onderzoek uit 2009 scoorde Nederland de 3e plaats. Nederland is het afgelopen jaar ingehaald door de Verenigde Staten (in 2009 de 5e plaats) en Finland (in 2009 de 10e plaats). Zweden en Denemarken scoorden zowel in 2009 als in 2010 beter dan Nederland.

De vijfde plaats van Nederland in het IBM onderzoek is als volgt opgebouwd:

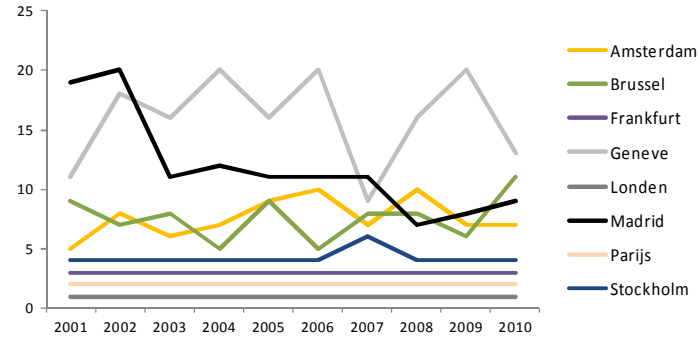
- *Connectiviteit ICT infrastructuur:* op dit punt staat Nederland na Zweden op de 2e plek wereldwijd.
- *Bedrijfsomgeving:* op het gebied van de bedrijfsomgeving neemt Nederland de 10e plaats in, achter landen als Singapore, Hong Kong, Zwitserland en Finland.
- *Sociaal culturele omgeving:* met betrekking tot de sociaal culturele omgeving scoort Nederland een 9e plaats, achter landen als de Verenigde Staten, Zweden, Denemarken en Finland.
- *Wet en regelgeving*: op het gebied van wet- en regelgeving komt Nederland uit op een gedeelde 5e plaats, samen met Nieuw Zeeland, Oostenrijk, België en Italië. Hong Kong, de Verenigde Staten, Singapore en Australië scoren beter op dit vlak dan Nederland.
- *Visie en beleid van de overheid:* Als het gaat om de visie en het beleid van de overheid scoort Nederland een 16e plaats. In deze categorie vallen punten als de digitale ontwikkelingsstrategie, de e-overheidsstrategie en de beschikbaarheid van online publieke dienstverlening voor burgers en bedrijven. De Verenigde Staten, Zuid Korea, Hong Kong en Singapore scoren erg hoog op dit vlak. Binnen Europa lopen vooral Zweden en Denemarken voorop.
- *Acceptatie en gebruik door consumenten:* Op dit punt scoort Nederland erg hoog en neemt de 1e plaats in.

51 *Bron: Digital economy rankings 2010, Beyond e-readiness, Economist Intelligence Unit & IBM, 2010.*

Amsterdam net buiten de Europese top 5 van beste telecomsteden
Uit onderzoek van Cushman & Wakefield (zie Figuur 5.4) naar de beste steden op het gebied van telecommunicatie, blijkt dat Amsterdam net buiten de top 5 van beste steden valt. Dat Amsterdam een aantrekkelijke vestigingsplaats voor ICT bedrijven is blijkt onder andere uit het aantal bedrijven dat in of rond Amsterdam hun datacenter vestigt. Ook Cisco noemt bij haar recente uitbreiding van activiteiten in Amsterdam de aantrekkelijke ICT infrastructuur in Nederland als belangrijke vestigingsreden.

Amsterdam laat een kleine daling zien in de periode 2001-2010. In 2001 nam het positie vijf in, in 2010 is het gedaald naar de zevende positie. Londen, Parijs en Frankfurt vormen in de periode 2001-2010 onveranderd de top 3. Ondanks dat telecommunicatie infrastructuur dus gezien wordt als één van de sterke punten van het Nederlands vestigingsklimaat, blijkt uit het onderzoek van Cushman & Wakefield (2010) dat er andere steden zijn die beter scoren op het gebied van telecommunicatie.

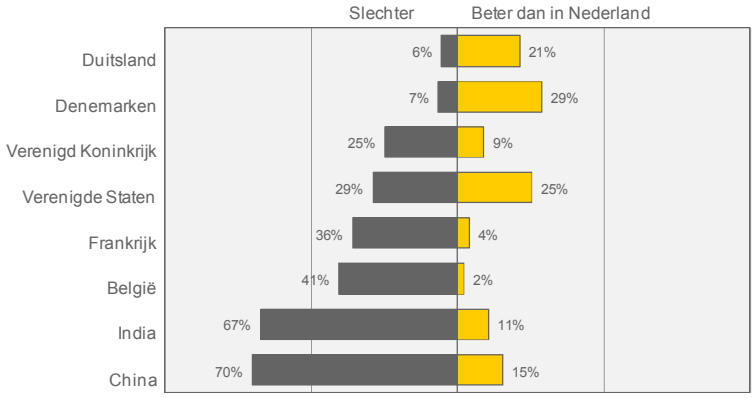
Figuur 5.4 Beste steden op het gebied van telecommunicatie, 2001-2010.



Bron: European Cities Monitor (2001-2010), Cushman & Wakefield, 2010.

Nederlandse bedrijven beoordelen veiligheid en betrouwbaarheid van de Nederlandse ICT infrastructuur als vergelijkbaar met of beter dan veel omliggende landen
In de ICT barometer hebben we directeuren, managers en professionals uit het Nederlandse bedrijfsleven gevraagd hoe zij de veiligheid en betrouwbaarheid van de ICT infrastructuur in de ons omliggende landen beoordelen in vergelijking met de veiligheid en betrouwbaarheid van de Nederlandse ICT infrastructuur. Daarbij blijkt dat Nederland het volgens de Nederlandse bedrijven het in vergelijking met andere landen niet slecht doet (zie Figuur 5.5). Nederlandse bedrijven hebben een hoge pet op van Denemarken en Duitsland, maar ze zijn aanzienlijk kritischer als het gaat om India en China. Ook in vergelijking met Frankrijk en België bestaat het beeld dat Nederland het beter doet op het gebied van de veiligheid en betrouwbaarheid van de ICT-infrastructuur.

Figuur 5.5 Wat is uw beeld van de veiligheid en betrouwbaarheid van de ICT-infrastructuur in onderstaande landen ten opzichte van Nederland? (gemiddeld 400 respondenten)



Bron: ICT barometer, Ernst & Young, 2010.

5.4 Belang van een veilige ICT infrastructuur als vestigingsplaatsfactor

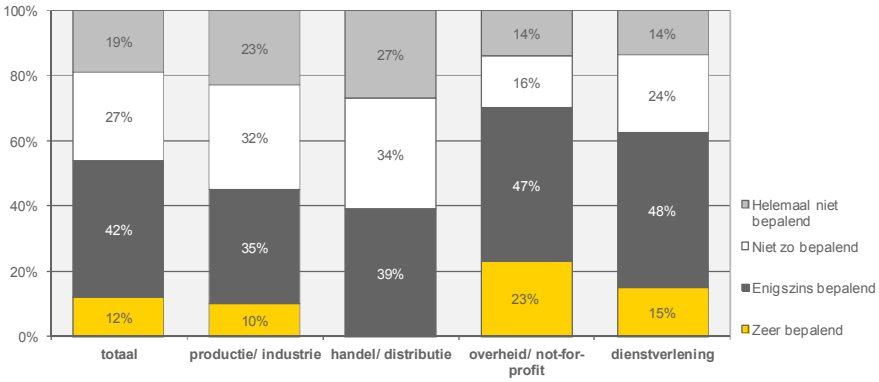
Kwaliteit van de telecominfrastructuur geldt als een belangrijke vestigingsplaatsfactor

In internationale vergelijkende onderzoeken wordt de kwaliteit van de telecominfrastructuur genoemd als een van de meest bepalende vestigingsplaatsfactoren. In de European Cities monitor van Cushman/Wakefield wordt dit na toegankelijkheid van markten en klanten en de beschikbaarheid van gekwalificeerd personeel als op twee na belangrijkste factor genoemd, vlak voor de kwaliteit van nationale en internationale transportverbindingen. De veiligheid en betrouwbaarheid van de ICT infrastructuur maakt een onderdeel uit van de kwaliteit van de totale telecominfrastructuur.

Vooral dienstverlenende organisaties beoordelen *veiligheid en betrouwbaarheid* van de ICT infrastructuur als belangrijk bij vestigingsbeslissingen

In de ICT Barometer hebben we directeuren, directeuren, managers en professionals van Nederlandse organisaties gevraagd in welke mate zij de veiligheid en betrouwbaarheid van de ICT infrastructuur een belangrijke factor vinden bij internationale vestigingsbeslissingen. Uit Figuur 5.6 blijkt dat ongeveer de helft van de respondenten dit als een enigszins tot zeer bepalende factor ziet. Respondenten uit de dienstverlenende sectoren beoordelen de veiligheid en betrouwbaarheid van ICT vaker als een belangrijke vestigingsplaatsfactor dan respondenten uit de productie/industrie en de handel/distributie.

Figuur 5.6 **Stel u bent betrokken bij het bepalen in welk land uw organisatie zich zal vestigen. In welke mate is veiligheid en betrouwbaarheid van ICT-infrastructuur een bepalende factor in uw keuze?**

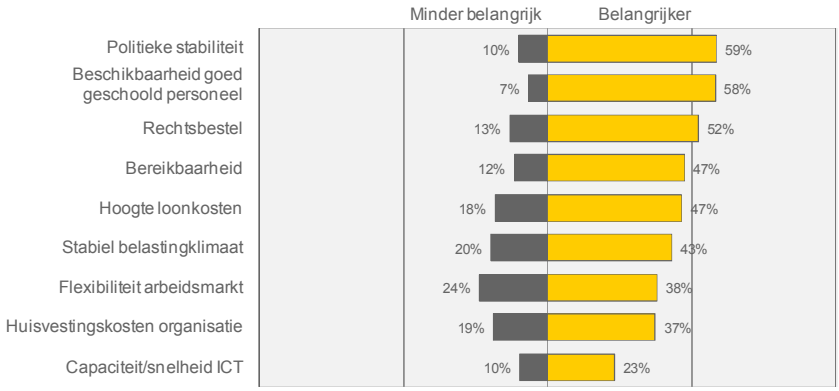


Bron: ICT barometer, Ernst & Young, 2010.

Andere factoren worden als belangrijker beoordeeld

In Figuur 5.7 is het belang van veilige en betrouwbare ICT-infrastructuur afgezet tegen andere locatiefactoren. Hoewel telecommunicatie infrastructuur als nummer drie wordt genoemd van de sterke punten van het Nederlands vestigingsklimaat, blijkt dat respondenten van de ICT Barometerbij de keuze voor een vestigingsplaats de ICT veiligheid niet opweegt tegen zaken als politieke stabiliteit, de beschikbaarheid van geschoold personeel en het rechtsbestel. Geïnterviewde brancheorganisaties en bedrijven voegen daar lokale vestigingsvoorwaarden (van gemeenten), internationaal afgestemde (fiscale) regelgeving en geografische ligging van afzetmarkten aan toe.

Figuur 5.7 **Hoe verhoudt het belang van een veilige en betrouwbare ICT-infrastructuur zich bij de keuze voor een vestigingsplaats in vergelijking met andere factoren? (gemiddeld 420 respondenten).**



Bron: ICT barometer, Ernst & Young, 2010.

Het beeld uit figuur 5.7 wordt bevestigd door vrijwel alle geïnterviewde partijen. Zij geven aan dat ICT veiligheid volgens hen alleen speelt als die vestigingsplaatsfactor onder een minimum niveau zou liggen. In Nederland is dat niet het geval. Het belang van de aanwezigheid van een veilige en betrouwbare ICT-infrastructuur kan per sector en per regio verschillen. De ICT-sector toont in Nederland een ruimtelijke concentratie in en rond Amsterdam. Hier bevindt zich ook één van de grote knooppunten in het Europese (glasvezel)kabelnetwerk. Daarnaast komt in de Eemshaven in Groningen de trans-Atlantische kabel van Tycom binnen, waar onder andere Google zich in het TCN datacenter heeft gevestigd.

NFIA en Amsterdam In Business, die beide bedrijven ondersteunen die zich in Nederland willen vestigen, geven aan dat zij vrijwel nooit vragen krijgen over de ICT veiligheid in Nederland.

Een aantal geïnterviewden geeft wel aan dat het minimale veiligheidsniveau langzaam naar boven verschuift. Ook wijzen zij er op dat de veiligheid en betrouwbaarheid wel een onderdeel vormt van de aantrekkelijkheid van het bredere ICT-klimaat. Het is vanuit dat oogpunt van belang om te blijven investeren in de veiligheid en betrouwbaarheid van de ICT infrastructuur. Wanneer er niet blijvend geïnvesteerd wordt in een voldoende veilig, betrouwbaar en toegankelijk ICT-netwerk, zal Nederland snel achterlopen.

5.5 Conclusie

Uit dit hoofdstuk komen de volgende conclusies naar voren:

- De kwaliteit van de ICT infrastructuur wordt door buitenlandse bedrijven gezien als een sterk punt van het Nederlandse vestigingsklimaat. Ook omliggende landen scoren echter goed op dit punt.
- De connectiviteit en de acceptatie en het gebruik van ICT door consumenten zijn internationaal gezien sterke punten van het Nederlandse ICT klimaat. De visie en het beleid van de overheid op het terrein van ICT wordt minder gewaardeerd. Het gaat dan om punten als de digitale ontwikkelingsstrategie, de e-overheidsstrategie en de beschikbaarheid van online publieke dienstverlening voor burgers en bedrijven.
- De veiligheid en betrouwbaarheid van de Nederlandse ICT infrastructuur is volgens Nederlandse bedrijven vergelijkbaar of beter dan in de meeste ons omringende landen. Denemarken en Duitsland worden gezien als landen waar de veiligheid en betrouwbaarheid nog wat hoger is dan in Nederland.
- De *veiligheid en betrouwbaarheid* van de ICT infrastructuur lijkt bij internationale vestigingsbeslissingen geen sterke bepalende factor te zijn. Uit het onderzoek komt het beeld naar voren dat zolang de veiligheid en betrouwbaarheid boven een minimumniveau blijft dit geen bepalende factor is bij een vestigingsbeslissing. Dat lijkt op dit moment het geval te zijn. In hoofdstuk 3 kwamen we echter wel tot de conclusie dat Nederlandse bedrijven relatief veel getroffen worden door ICT-veiligheidsincidenten. . De veiligheid en betrouwbaarheid vormen wel een belangrijk onderdeel van de aantrekkelijkheid van het bredere ICT-klimaat. Het is dus wel van belang om te voorkomen dat Nederland onder het minimumniveau zakt (de lat komt steeds hoger te liggen). Aandacht voor ICT-veiligheid blijft dus ook vanuit het vestigingsklimaat van belang.

6 Conclusies en aanbevelingen

6.1 Inleiding

In dit rapport is zijn de resultaten gepresenteerd van een onderzoek naar de bijdrage van een betrouwbare en veilige ICT-infrastructuur voor de duurzame economische groeikansen van Nederland.

In het onderzoek stonden de volgende onderzoeksvragen centraal:

1 *In welke mate draagt een veilige en betrouwbare ICT-infrastructuur bij aan het Nederlandse vestigingsklimaat en aan duurzame economische groei in Nederland?*
   a. *Wat is de (potentiële) relatieve bijdrage van (veilige en betrouwbare) ICT aan de economische groeikansen van Nederland?*
   b. *Wat is de relatieve betekenis van (veilige en betrouwbare) ICT bij de vestigingsplaatskeuze van bedrijven en hoe scoort Nederland ten opzichte een aantal relevante andere landen op het terrein van veilige ICT als vestigingsplaatsfactor?*
   c. *Wat is de (meer)waarde van vertrouwen in de ICT-sector en specifiek in relatie tot veilige netwerken en informatiebeveiliging aan de kant van de eindgebruiker?*

Gezien de beperkte doorlooptijd en de brede vraag die aan het onderzoek ten grondslag lag, is er bij de start veel aandacht besteed aan de afbakening van het onderzoek. Daarbij is in overleg met de opdrachtgever besloten het onderzoek te focussen op drie belangrijke elementen die bepalend zijn voor de bijdrage van een betrouwbare en veilige ICT-infrastructuur aan de duurzame economische groeikansen van Nederland:

- De directe schade door veiligheids- en betrouwbaarheidsproblemen bij het bedrijfsleven in termen van productieverlies;
- De betekenis van een veilige en betrouwbare ICT-infrastructuur voor het Nederlandse vestigingsklimaat;
- De (meer) waarde van vertrouwen in de ICT aan de kant van de eindgebruiker (zakelijk en consumenten).

2 *Hoe kan ons land zich op het terrein van ICT-veiligheid en -betrouwbaarheid onderscheiden van andere landen/EU lidstaten?*
   a. *Waarin kan Nederland zich onderscheiden en waarin moet Nederland juist samen optrekken met andere (EU-lid)staten met betrekking tot een veilige/betrouwbare ICT-infrastructuur in relatie tot economische groeimogelijkheden en vestigingsklimaat*[52]*?*

[52] *Gedacht wordt in eerste instantie aan extra veiligheidsbeleid en/of inspanningen van marktpartijen.*

b. *Specifiek op ICT-veiligheidsterrein: Is veiligheid van netwerken/ informatiebronnen en vertrouwen vooral afhankelijk van grote incidenten of meer van dagelijkse vervelende hinder?*

Hieronder werken wij de belangrijkste conclusies van het onderzoek uit. Daarbij nemen wij de onderzoeksvragen als uitgangspunt (paragraaf 7.3). Het hoofdstuk wordt afgesloten met een aantal aanbevelingen van de onderzoekers voor toekomstig beleid van de Nederlandse overheid op het terrein van ICT veiligheid vanuit een economisch perspectief (paragraaf 7.3).

6.2 Conclusies

1 *In welke mate draagt een veilige en betrouwbare ICT-infrastructuur bij aan het Nederlandse vestigingsklimaat en aan duurzame economische groei in Nederland?*

De waarde van minder directe schade bij het bedrijfsleven
Het Nederlandse bedrijfsleven is wat betreft haar bedrijfsprocessen steeds meer afhankelijk van ICT. Daarbij wordt steeds meer gebruik gemaakt van internet voor bijvoorbeeld het ontvangen van orders, betalingsverkeer, faciliteren van thuiswerken, gegevensuitwisseling. Nederland beschikt over een hoogwaardig netwerk met een relatief hoge penetratie van breedbandverbindingen.

Een dergelijk hoogwaardig netwerk brengt ook kwetsbaarheden met zich mee. Voor Nederlandse bedrijven betekenen deze kwetsbaarheden dat zij geconfronteerd kunnen worden met ICT-gerelateerde veiligheids- en betrouwbaarheidsproblemen[53]. In vergelijking met andere Europese landen worden Nederlandse bedrijven relatief veel getroffen door dergelijke problemen.

Het wegvallen van de netwerkverbinding en de infectie van systemen door malware zijn veel voorkomende ICT-problemen, met volgens bedrijven een grote potentiële impact op de bedrijfsvoering. De diefstal van vertrouwelijke gegevens, een denial of service aanval en phishing komen veel minder vaak voor, maar hebben (wanneer zij voorkomen) wel een grote impact op de bedrijfsvoering.

In dit onderzoek hebben wij een globale inschatting gemaakt van de omvang van een deel van de directe schade die bedrijven ondervinden als gevolg van ICT-veiligheidsincidenten. In termen van kansen geeft het onderzoek een eerste beeld van de kostenbesparingen die op deze gebieden (in potentie) mogelijk zijn voor Nederlandse bedrijven wanneer de betrouwbaarheid en de veiligheid van de ICT infrastructuur (verder) verbetert. Het onderzoek is daarbij geenszins volledig. Dit zou een veel groter en omvangrijker onderzoek vereisen.

Uit onderzoek van Ernst & Young naar cybercrime komt naar voren dat 1 op de drie bedrijven in Nederland in 2010 schade heeft ondervonden als gevolg van cybercrime. Een op de vijf bedrijven leed hierdoor ook directe financiële schade.

53 *Zo blijkt uit een recente studie van de TU Delft dat in Nederland tussen de 450.000 en 900.000 computers besmet en onderdeel zijn van botnets. De geïnfecteerde computers worden gebruikt om grote hoeveelheden spam te verspreiden en in toenemende mate ook voor identiteitsdiefstal en aanvallen op websites van bedrijven. Bron: TU Delft en Michigan State University, Internet Service Providers and Botnet Migitation, A factfinding study on the Dutch market, Januari 2011.*

De omvang van deze financiële schade varieert per bedrijf (van minder dan 10.000 euro tot meer dan 1 miljoen euro). De omvang van deze directe financiële schade voor de Nederlandse economie is aanzienlijk.

In het onderzoek is verder ingezoomd op twee directe schadeposten voor het bedrijfsleven:

- het productieverlies als gevolg van netwerkuitval;
- het productieverlies als gevolg van ontvangen en verwerken van spam.

Uit tabel 6.1 blijkt dat het beperken van de tijd die werknemers bezig zijn met het lezen en verwerken van spam belangrijke economische kansen biedt. Wij schatten deze schadepost voor 2010 in op 1 tot 2 miljard euro. Dat is 150 tot 300 euro per werknemer per jaar. Opvallend is dat spam door bedrijven wel gezien wordt als een veel voorkomend probleem, maar niet als een probleem dat een grote impact heeft op de bedrijfsvoering. Vooral binnen kleinere bedrijven zijn werknemers per dag relatief veel tijd kwijt met de verwerking van spam. Met name hier liggen dan ook kansen voor verbetering.

Tabel 6.1 Overzicht globale inschatting productieverlies in Nederland als gevolg van netwerkuitval en spam – 2010.

	Door oorzaken van buiten de eigen organisatie	Door oorzaken binnen de eigen organisatie
Productieverlies door netwerkuitval	100-150 mln. euro	200-300 mln. euro
Productieverlies als gevolg van spam	1 – 2 mld. euro	N.v.t.
Totaal productieverlies als gevolg van netwerk-uitval en spam	**1,1 – 2,2 mld. euro**	**0,2 – 0,3 mld. euro**

In het onderzoek hebben wij ingezoomd op twee schadeposten. Andere belangrijke schadeposten zoals de schade door digitale diefstal van vertrouwelijke informatie (klantgegevens, inlogcodes, bedrijfsgegevens), het omzetverlies bij bedrijven als gevolg van het tijdelijk niet beschikbaar zijn van de website en de schade als gevolg van diefstal van vertrouwelijke informatie zijn niet verder uitgewerkt in het onderzoek. Er is niet voldoende informatie bekend om (binnen dit onderzoek) tot een goede inschatting te komen van de absolute omvang van deze schadeposten. Bekend is wel dat de schade voor financiële instellingen als gevolg van fraude met internetbankieren (o.a. phishing) in de eerste helft van 2010 volgens de banken 4,3 mln. euro bedroeg. Ook cascade-effecten (door de toenemende verknoping van netwerken en de toenemende afhankelijkheid van de economie van ICT) zijn buiten beschouwing gelaten. Om het beeld verder in te vullen is verder onderzoek nodig.

Naast de schade die het bedrijfsleven ondervindt als gevolg van ICT betrouwbaarheids- en veiligheidsproblemen doen zij ook investeringen om dergelijke problemen te voorkomen. Uit ons onderzoek komt naar voren dat bedrijven en non-profitorganisaties in 2010 gemiddeld 17 procent van hun totale ICT-budget besteden aan ICT veiligheid[54].

54 *Daarnaast doen ook consumenten, de netwerkserviceproviders en de overheid investeringen om de ICT veiligheid te verhogen. Deze zijn in dit onderzoek niet in beeld gebracht.*

De economische (meer)waarde van vertrouwen bij de eindgebruiker
Het vertrouwen van consumenten en bedrijven in de veiligheid en betrouwbaarheid van de Nederlandse ICT-infrastructuur is een bepalende factor voor het gebruik dat zij maken van die infrastructuur. Bij vertrouwen gaat het daarbij om verschillende aspecten, zoals het vertrouwen dat er geen misbruik wordt gemaakt van persoonlijke en vertrouwelijke gegevens, vertrouwen dat de privacy niet geschonden wordt, vertrouwen dat financiële transacties op een veilige manier plaatsvinden en vertrouwen dat goederen en diensten die online worden besteld ook geleverd worden. Ook het vertrouwen in de beschikbaarheid is van belang.

Vertrouwen bij het bedrijfsleven
Uit ons onderzoek komt naar voren dat Nederlandse bedrijven een groot vertrouwen hebben in de ICT-beveiliging van de eigen organisatie. Ruim 80% heeft hier veel vertrouwen in. Tegelijkertijd geeft vier op de tien bedrijven aan zich als gevolg van veiligheidsissues beperkingen op te leggen in het gebruik van de technische mogelijkheden op het terrein van ICT. Gevolg hiervan is dat veel bedrijvenniet of niet volledig gebruik maken van de (technische) mogelijkheden om de dienstverlening aan de klant te digitaliseren of om informatiestromen te digitaliseren. Het gebruik van dergelijke technische mogelijkheden biedt kansen voor bedrijven om productiviteitsvoordelen te behalen. Adequate beveiliging is hierbij vanzelfsprekend randvoorwaardelijk.

Uit het onderzoek komen twee belangrijke uitdagingen naar voren:
1 Versterken van het vertrouwen van bedrijven in de ICT infrastructuur. Uit ons onderzoek komt naar voren dat managers en professionals binnen Nederlandse bedrijven de veiligheid van de Nederlandse ICT infrastructuur beoordelen met het rapportcijfer 6,7 en de betrouwbaarheid een 6.9. Dit rapportcijfer laat zien dat, hoewel de grondhouding positief is, er volgens de bedrijven nog zeker ruimte is voor verbetering. Die ligt bijvoorbeeld in de verbetering van de controleerbaarheid van de datastromen. Dit kwaliteitsaspect krijgt het laagste rapportcijfer: een 6,3.
2 Meer inzicht in kosten en voordelen van verdere investeringen: Het grote vertrouwen van bedrijven in de eigen ICT beveiliging heeft als risico dat het een belemmering kan vormen voor het verder benutten van de kansen op verdere productiviteitsverbetering. Dat is het geval wanneer men terecht inschat dat er hiervoor een nog hoger beveiligingsniveau noodzakelijk is, maar dat dit technisch niet mogelijk is of dat dit forse investeringen vereist (men investeert immers al veel in beveiliging). Een belangrijke uitdaging ligt in dat geval in een realistische beeldvorming van het beveiligingsniveau van de eigen organisatie van bedrijven en van de voordelen van het investeren in de kansen die ICT nog biedt en de daarbij behorende kosten, waaronder beveiligingskosten.

Vertrouwen bij consumenten
Op basis van een doorvertaling van een Europese analyse van Booz & Co naar het Nederlandse niveau, schatten wij in dat in Nederland een versterking van het vertrouwen in het internet bij de Nederlandse consument in 2014 potentieel tot (bruto) 1,2 miljard meer omzet aan verkopen van producten en diensten via internet kan leiden. Deze extra groei in internetverkopen kan voortkomen uit een toename van het bestede bedrag van consumenten die ook op dit moment al online aankopen doen, maar ook uit de groep consumenten die dit op dit moment nog niet doet, omdat zij bezorgd is over de veiligheid van online betalingstransacties. Bij beide groepen ligt potentie.

Voor de groep Nederlandse consumenten die al wel online producten of diensten koopt, geldt dat deze potentie kan worden gerealiseerd door het bestede bedrag per consument te verhogen. Het bestede jaarlijks bedrag per consument is in vergelijking met andere Europese landen relatief laag. In 2009 gaf de Nederlandse consument ruim 800 euro uit, terwijl Deense en Britse consumenten meer dan 1200 euro uitgaven. In 2009 maakte de online omzet uit de verkoop van producten en diensten via het internet (e-commerce) ongeveer 1% uit van de totale Nederlandse economie. Daarmee blijft Nederland achter op een aantal andere EU-landen, zoals het Verenigd Koninkrijk en Denemarken waar e-commerce rond de 2% van de economie uitmaakt (zie tabel 6.2).

Tabel 6.2 Benchmark Europese landen op het terrein van "online verkoop" (2009).

	Percentage online consumenten	Online verkoop per consument (in €)	Online verkoop (in mld. €)	Online verkoop als % BNP
Verenigd Koninkrijk	66%	1239,51	42,7	1,98%
Denemarken	64%	1213,25	3,9	1,92%
Finland	54%	975,56	2,6	1,41%
Noorwegen	-	1101,69	3,3	1,30%
Frankrijk	45%	994,65	24,7	1,19%
Duitsland	56%	764,98	33,4	1,19%
Nederland	***63%***	***857,00***	***7,4***	***1,16%***
Zweden	63%	801,79	3,8	1,13%
Spanje	23%	778,65	6,3	0,47%
Italië	12%	934,67	8,2	0,45%

Bron: Eurostat, Kelkoo, CIA World Factbook, Thuiswinkel.org

Hoewel de oorzaak van het verschil in het bestede bedrag per consument niet direct gelegen is in vertrouwensaspecten, biedt het versterkt inzetten op meer vertrouwen in de veiligheid van internet bij consumenten wel mogelijkheden om deze achterstand in te lopen.

Naast de groep die al wel online koopt is er een omvangrijke groep van ongeveer één miljoen consumenten die op dit moment geen producten online aanschaft, (onder andere) omdat zij geen vertrouwen hebben in de veiligheid van online betalingstransacties. Zouden al deze consumenten dit wel doen en ook hetzelfde bedrag besteden als de gemiddelde online consument dan levert dat 900 miljoen euro aan extra online omzet op. Of deze potentie wordt benut hangt onder andere af van andere bezwaren die deze consumenten eventueel hebben bij het kopen op internet.

Een van de opvallende conclusies uit hoofdstuk 4 is dat consumenten zich relatief veel zorgen maken over misbruik van persoonlijke gegevens, schending van privacy en financiële schade door phishing of fraude met betaalmiddelen, terwijl maar een zeer klein deel van de consumenten daar zelf door getroffen wordt. Een belangrijke uitdaging ligt er dan ook in om consumenten meer vertrouwen te geven dat er goed met hun gegevens wordt omgegaan en dat betalen via internet veilig is.

Tegenover de economische potentie van een hoger vertrouwen staat een potentieel economisch risico wanneer het vertrouwen afneemt. In de interviews wordt er op gewezen dat dit risico qua omvang in potentie groter is dan de huidige directe schade die bedrijven op dit moment ondervinden als gevolg van ICT veiligheidsproblemen. Booz & Co schat in haar analyse in dat dit risico in economische termen een omvang heeft van ongeveer tweemaal de extra economische potentie bij een toename van het vertrouwen.

De (meer)waarde voor het vestigingsklimaat

Uit ons onderzoek komt naar voren dat Nederland beschikt over een kwalitatief hoogwaardige ICT-infrastructuur. Op vestigingsplaatslijstjes staat Nederland op het terrein van de aantrekkelijkheid van ICT en Telecom in de Europese top 5. Dat is belangrijk, want de kwaliteit van de telecom infrastructuur wordt in internationale onderzoeken genoemd als een van de drie meest bepalende vestigingsplaatsfactoren. De hoogwaardige ICT en Telecom infrastructuur levert dus een belangrijke bijdrage aan de aantrekkingskracht van Nederland op buitenlandse bedrijven.

De *veiligheid en betrouwbaarheid* van de ICT-infrastructuur vormt weliswaar een belangrijk onderdeel van de kwaliteit van de Nederlandse ICT-infrastructuur, maar lijkt op dit moment voor bedrijven die een beslissing nemen over een nieuwe vestigingsplaats geen doorslaggevende factor bij deze beslissing. Andere factoren, zoals politieke stabiliteit, de beschikbaarheid van geschoold personeel en het rechtsbestel, maar ook de snelheid van ICT verbindingen spelen een grotere rol.

Uit het onderzoek komt het beeld naar voren dat veiligheid en betrouwbaarheid van de ICT-infrastructuur vooral op de achtergrond een rol speelt. Er is een minimaal noodzakelijk niveau van veiligheid en betrouwbaarheid van de ICT-infrastructuur nodig. Ligt het niveau onder dit minimum niveau dan geldt het als een negatieve vestigingsplaatsfactor, maar ligt het niveau boven het minimum dan lijkt een nog hoger niveau voor vestigingsplaatsbeslissingen (op enkele specifieke typen bedrijvigheid na) geen grote rol meer te spelen en zijn andere factoren belangrijker. Nederland voldoet volgens de partijen die wij in het onderzoek hebben geïnterviewd op dit moment ruimschoots aan dit niveau. Tegelijkertijd blijkt uit cijfers van Eurostat dat relatief veel Nederlandse bedrijven in 2009 getroffen werden door ICT veiligheidsincidenten. Dat het op dit moment niet speelt betekent dus niet dat er geen blijvende aandacht nodig is.

Wanneer we Nederland vergelijken met het Verenigd Koninkrijk, België en Duitsland, blijkt dat ook voor deze landen de ICT-infrastructuur als een aantrekkelijke factor wordt gezien. Op het gebied van veiligheid en betrouwbaarheid van de ICT-infrastructuur worden vooral Denemarken en Duitsland hoog gewaardeerd. Nederland doet het beter dan landen als India en China en Nederlandse managers en ICT-professionals zijn ook positiever over Nederland ten opzichte van Frankrijk en België. Wanneer we Nederland internationaal vergelijken op het gebied van andere ICT gerelateerde factoren die invloed hebben op de mate waarin consumenten, bedrijven en de overheid in staat zijn de voordelen van de aanwezige ICT-infrastructuur te benutten, blijkt dat in Europa vooral Zweden, Denemarken, Finland en Zwitserland hoog scoren. Hoewel Nederland ook hoog scoort op een aantal van deze factoren is Nederland de laatste jaren gedaald in de internationale ranglijsten. Daarbij valt op dat Nederland vooral laag scoort op de visie en het beleid van de overheid op het gebied van de elektronische overheid. Nederland scoort daarentegen hoog op de acceptatie en gebruik bij bedrijven en consumenten van ICT.

Nederland doet het dus wat betreft de locatiefactor veiligheid en betrouwbaarheid van ICT-infrastructuur goed in vergelijking met andere landen, maar het is niet uniek op het gebied van veilige en betrouwbare ICT-infrastructuur en aandacht blijft noodzakelijk.

1 Hoe kan ons land zich op het terrein van ICT veiligheid /betrouwbaarheid onderscheiden van andere landen/EU lidstaten?

Waarop onderscheiden en waarop juist samen optrekken?
Nederland beschikt over een kwalitatief hoogwaardige ICT- en telecominfrastructuur. Dit blijkt uit meerdere onderzoeken, o.a. uitgevoerd door IBM, Cisco en Ernst & Young. Wat betreft de veiligheid en betrouwbaarheid van de ICT-infrastructuur bestaat bij in Nederland gevestigde bedrijven het beeld dat dit goed is geregeld ten opzichte van andere landen. Toch is blijvende aandacht wel noodzakelijk. Nederlandse bedrijven worden in vergelijking met bedrijven in andere Europese landen vaker getroffen door ICT-veiligheidsincidenten. Ook waarderen Nederlandse bedrijven de veiligheid en betrouwbaarheid van de Nederlandse ICT infrastructuur met een '7-min'. Dat is op zich zelf geen slecht rapportcijfer, maar laat ook zien dat er nog ruimte is voor verbetering.

Hiervoor is reeds geconcludeerd dat vanuit het perspectief van het vestigingsklimaat geldt dat wanneer Nederland haar relatieve positie op het terrein van ICT-veiligheid ten opzichte van andere landen verbetert, dit waarschijnlijk niet zal leiden tot een verbetering van het vestigingsklimaat. Dat betekent niet dat Nederland niet in ICT-veiligheid moet investeren. De lat komt steeds hoger te liggen en eerder in dit rapport concludeerden we al dat er wel degelijk een aantal aandachtspunten is. Samen optrekken met andere landen of in EU verband bij de aanpak van ICT-veiligheids- en betrouwbaarheids-problemen ligt voor de hand. Het internet is een internationaal netwerk waarin landsgrenzen nauwelijks een rol spelen. Datzelfde geldt voor de toepassingen van het internet. Bedrijven maken bijvoorbeeld gebruik van datacenters in het buitenland. Data van consumenten en bedrijven worden opgeslagen op servers in het buitenland. Phishing, verspreiding van spam en virusaanvallen hebben vaak een internationaal karakter[55].De veiligheidsuitdagingen die deze ontwikkelingen met zich meebrengen kunnen alleen door internationale samenwerking effectief worden aangepakt[56].

Vanuit het economische groeiperspectief komen er uit het onderzoek voor Nederland vooral uitdagingen naar voren op het terrein van vertrouwen van consumenten in de veiligheid van internet en in de bestrijding van spam.

Met betrekking tot de bestrijding van spam is vooral bij bedrijven in het MKB nog verbetering mogelijk. Ondanks de beperkte door de bedrijven zelf gepercipieerde impact betekent de paar minuten derving in arbeidstijd per werknemer per dag door spam op jaarbasis en op het niveau van de hele Nederlandse economie een omvangrijke belasting.

Het verhogen van het vertrouwen in internet bij consumenten kan in potentie ook een belangrijke impuls geven aan de digitale (binnenlandse) economie. Ook richting het buitenland zou Nederland zich op dit punt kunnen onderscheiden.

---

55 *KLPD, Overallbeeld Aandachtsgebieden, juli 2010.*

56 *Zie bijvoorbeeld de speech van Eurocommissaris Kroes op de 'Les Assises du Numérique' conference in Parijs: 'Cloud Computing and Data Protection' over het belang van een Europese regelgeving rond data protection, 25 november 2010.*

Daarmee kan mogelijk nieuwe buitenlandse bedrijvigheid worden aangetrokken. Wat betreft het vertrouwen in internettransacties behoort Nederland tot de top van Europa. Er is nog wel een inhaalslag nodig bij de groep consumenten die op dit moment vanwege vertrouwen in de veiligheid en privacyaspecten nog geen aankopen via internet doet. Dit aandeel is in Nederland nog relatief hoog.

Grote incidenten versus dagelijkse hinder

Bedrijven
Uit ons onderzoek komt naar voren dat bedrijven het afgelopen jaar vooral hinder hebben ondervonden van trage of weggevallen netwerkverbindingen en het ontvangen van spam. Uit ons onderzoek komt naar voren dat spam door veel bedrijven weliswaar wordt gezien als een minder belangrijk probleem, maar dat de dagelijkse hinder van spam in termen van productieverlies toch een behoorlijke impact heeft.

Consumenten
Net zoals bedrijven hebben consumenten veel last van het ontvangen van ongewenste e-mailberichten. Daarnaast hebben zij vooral last van computervirusinfecties. Hoewel consumenten hier veel minder door getroffen worden, maken zij zich ook bezorgd over het misbruik van persoonlijke gegevens of schending van privacy en fraude met betaal- of creditcards. Deze lijken bepalend voor het vertrouwen van consumenten.

6.3 Aanbevelingen

Behoud en versterk het goede
In dit rapport staan de economische kansen van een veilige en betrouwbare ICT infrastructuur centraal. Of deze economische kansen ook gerealiseerd worden hangt enerzijds af van de mate waarin de veiligheid en betrouwbaarheid (ondanks de toenemende complexiteit) kan worden behouden en verstevigd. Anderzijds is het vertrouwen van consumenten en bedrijven van groot belang om de kansen te benutten.

Maatregelen van de overheid en de marktpartijen zijn ook op dit moment al gericht op het versterken van de veiligheid en betrouwbaarheid en het vertrouwen bij de eindgebruiker. Wij bevelen aan deze maatregelen te handhaven en verder te versterken[57]. Deze maatregelen vormen een basisvoorwaarde om de uitdagingen die uit ons onderzoek naar voren komen te realiseren:

- *De bestrijding van Cybercrime:* de aanpak van cybercrime is een speerpunt van het kabinetsbeleid. Een effectieve aanpak van cybercriminaliteit beperkt de schade en verhoogt het vertrouwen bij eindgebruikers.
- *Betrouwbaarheid en continuïteit van het hoofdnetwerk:* Door de nog steeds sterk in omvang toenemende datastromen en de daaraan gekoppelde toenemende behoefte aan bandbreedte staat de betrouwbaarheid en continuïteit steeds onder druk. De verantwoordelijkheid hiervoor ligt overigens in eerste instantie bij de netwerkaanbieders.

---

57 *Daarbij gaat het uiteraard wel steeds om een afweging tussen veiligheid en innovativiteit. Te stringent beleid en regelgeving rond ICT veiligheid kan innovatie en bedrijvigheid ook belemmeren, doordat bijvoorbeeld diensten daardoor niet geleverd kunnen worden of doordat daardoor consumenten zich in hun privacy aangetast voelen.*

- *Communicatie over risico's en voordelen van internetgebruik:* Programma's als Digibewust, Veilig Internetten en Veilig Bankieren zetten hier op in.

Naast het behoud en het versterken van maatregelen die ook nu reeds worden genomen doen wij de volgende aanbevelingen.

Investeer in het terugdringen van spam in het MKB
Door bedrijven wordt spam niet gezien als een probleem met een grote invloed op de bedrijfsvoering. Uit ons onderzoek blijkt echter dat de dagelijkse last op jaarbasis een behoorlijke kostenpost oplevert. Vooral in het MKB is de last hoog. Dat komt mogelijk doordat het MKB veelal werkt met minder goede spamfilters. Voorlichting richting het MKB over de kosten en baten van een goede spambestrijding kan per saldo voor bedrijven veel efficiencywinst opleveren.

Maak bedrijven meer bewust van de eigen verantwoordelijkheid, maar biedt ook hulp om die op te pakken
De veiligheid van de ICT infrastructuur wordt voor een belangrijk deel niet bepaald door de veiligheid van het hoofdnetwerk zelf, maar door de beveiliging van de netwerkaansluitingen op dit hoofdnetwerk. Uit ons onderzoek komt het beeld naar voren dat bedrijven veel vertrouwen hebben in de eigen beveiligingsmaatregelen. Tegelijkertijd worden Nederlandse bedrijven relatief veel geconfronteerd met ICT veiligheidsincidenten. Een verbetering van het bewustzijn van de eigen verantwoordelijkheid en van de werkelijke kwaliteit van de eigen beveiligingsmaatregelen kan de veiligheid van de ICT infrastructuur bevorderen.

Ook aan de kant van de betrouwbaarheid en continuïteit van de ICT infrastructuur geldt een eigen verantwoordelijkheid voor bedrijven. Met netwerkaanbieders kunnen afspraken gemaakt worden over gegarandeerde betrouwbaarheids-/continuïteitsniveaus (in de vorm van SLA's). Het is vooral een kosten-baten afweging voor bedrijven of zij bereid zijn om voor deze grotere betrouwbaarheid/continuïteit te betalen. De baten zijn veelal echter moeilijk te kwantificeren omdat het vaak gaat om het voorkomen van schade.

Tegelijkertijd worden de risico's en de te nemen maatregelen om die risico's te beperken steeds complexer. Voor (kleinere) bedrijven is dit steeds moeilijker te overzien. Er is daarom in toenemende mate ook een rol weggelegd voor bijvoorbeeld service providers, financiële dienstverleners, de aanbieders van online diensten om bedrijven daarin te ondersteunen door het (gratis of tegen vergoeding) bieden van oplossingen of voorlichting.

Geef het bedrijfsleven inzicht in kosten en baten van nog bestaande productiviteitsverbeteringen
Uit het onderzoek komt naar voren dat bedrijven ondanks een hoog vertrouwen in de eigen ICT beveiliging toch mogelijkheden tot bijvoorbeeld verdere digitalisering van diensten aan klanten of digitalisering van informatiestromen onbenut laten vanwege veiligheidsredenen. Mogelijk denken bedrijven dat er geen technische mogelijkheden zijn om de veiligheidsbelemmeringen die zij zien weg te nemen of hebben zij het beeld dat hier omvangrijke investeringen voor nodig zijn die niet opwegen tegen de voordelen van deze investeringen in termen van toegenomen productiviteit of toename van de omzet. Voorlichting over mogelijkheden hiertoe, de kosten hiervan, maar ook baten kan bedrijven het vertrouwen geven om verder te investeren in ICT mogelijkheden.

Versterk de controleerbaarheid van datastromen over de infrastructuur voor bedrijven
Bedrijven beoordelen de controleerbaarheid van de ICT infrastructuur als matig (een rapportcijfer 6,3). Het gaat daarbij om de mate waarin te controleren is of gegevens juist, volledig en tijdig zijn uitgewisseld. En: de mate waarin de oorzaak te achterhalen is wanneer dit niet het geval is. Het vertrouwen van Nederlandse bedrijven in de Nederlandse ICT infrastructuur kan versterkt worden door de controleerbaarheid van datastromen te versterken. Wij bevelen dan ook aan samen met de service providers te onderzoeken hoe de controleerbaarheid voor bedrijven verbeterd kan worden.

Verhoog het vertrouwen van consumenten in de veiligheid en privacy van persoonsgegevens op internet
Voor ongeveer een kwart van de consumenten die nog geen online aankopen doen spelen privacyaspecten hierbij een belangrijke rol. Door consumenten meer zekerheid te bieden dat de veiligheid en de privacy van de gegevens die zij achter laten gegarandeerd is kan het vertrouwen van consumenten in internet verder worden versterkt. Een mogelijkheid hiertoe is om in de bestaande keurmerken het privacybeleid te versterken of meer naar voren te brengen in de communicatie.

Zorg voor meer helderheid over de betrouwbaarheid van internetbedrijven
Meer helderheid in de betrouwbaarheid van internetwinkels kan het vertrouwen van consumenten verder versterken. Diverse keurmerken hebben tot doel om deze betrouwbaarheid te garanderen. Mogelijkheden liggen bijvoorbeeld in het versterken van deze keurmerken (uitbreiden criteria voor deelname), of harmonisatie (samenvoegen keurmerken). Samen met de aanbieders van de keurmerken kan onderzocht worden hoe de overheid hier een bijdrage aan kan leveren.

Onderzoek mogelijkheden wegnemen risico's bij de consument
Ter versterking van het vertrouwen in de ICT infrastructuur bij consumenten kunnen naast communicatie ook andere middelen worden ingezet. Een alternatieve maatregel zou bijvoorbeeld kunnen liggen in het verschuiven van het risico op schade van de consument naar de internetdienstverlener. Dat kan bijvoorbeeld door consumenten een financiële compensatie te geven wanneer zij buiten hun schuld om worden geconfronteerd met veiligheidsproblemen, financiële schade, of netwerkuitval. Een dergelijke compensatie is in de luchtvaart en in het spoorvervoer al gebruikelijk. Op het terrein van internet is dit ook niet helemaal nieuw. Zo vergoeden banken skimming en phishing incidenten de schade aan consumenten. Ook worden in SLA's van internetserviceproviders op de business-to-business markt afspraken gemaakt over vergoedingen bij een te lage beschikbaarheid van het netwerk. Deze methodiek is ook op bredere schaal denkbaar, bijvoorbeeld door consumenten een vergoeding te bieden bij een (verwijtbare) storing van de internetverbinding, of door een vergoeding te geven voor schade van het niet-(tijdig) leveren van internetaankopen. Een ander voorbeeld van een dergelijke regeling is de ontwikkeling van een garantiefonds voor internetwinkels, die consumenten de garantie van levering biedt, ook wanneer de oorspronkelijke aanbieder niet in staat is om te leveren of weigert aan de aangegane verplichting te voldoen. Nader onderzoek kan uitwijzen of een dergelijke aanpak effectief is.

Werken aan vertrouwen en veiligheid vereist samenwerking en een heldere regie

Bij het op peil houden en versterken van de betrouwbaarheid en veiligheid van de Nederlandse ICT infrastructuur en het vertrouwen bij de eindgebruiker hier in zijn vele partijen betrokken (netwerkaanbieders, overheid, financiële dienstverleners, aanbieders van diensten). Hoewel er tussen deze partijen al we samengewerkt wordt, willen wij het belang van een verdere versterking van de samenwerking hier onder de aandacht brengen. Alleen vanuit een gezamenlijke visie en afstemming van activiteiten gericht op de verbetering van ICT veiligheid over de partijen heen kan de economische potentie van een groter vertrouwen bij bedrijven en consumenten in de ICT veiligheid volledig worden gerealiseerd. Uit de gesprekken die wij in het kader van het onderzoek hebben gevoerd met vertegenwoordigers van de verschillende partijen komt het beeld naar voren dat de samenwerking nog verder kan worden versterkt. Voor de overheid is in dit verband eventueel een faciliterende rol weggelegd.

Overigens liggen er op dit punt ook nog uitdagingen binnen de rijksoverheid zelf. De overheidsverantwoordelijkheden op het terrein van ICT veiligheid zijn verspreid over verschillende departementen. In ons onderzoek is door meerdere partijen aangegeven dat een dergelijke spreiding van verantwoordelijkheden, deels met overlappende taakvelden weinig bevorderlijk werkt voor een eenduidig duidelijk beleid vanuit de overheid op het terrein van ICT veiligheid. Van belang is om de coördinerende rol goed op te pakken, de rollen en verantwoordelijkheden van de departementen scherper te definiëren, en strak binnen de eigen rol en verantwoordelijkheid te opereren.

Aanbevelingen voor verder onderzoek

In dit rapport staat de (meer)waarde van een veilige en betrouwbare ICT infrastructuur voor de Nederlandse economie centraal. Bij de start van het onderzoek was reeds duidelijk dat deze studie geen volledig antwoord zou kunnen geven. De problematiek rond ICT veiligheid en de doorwerking daarvan in de economie is dusdanig complex dat hiervoor een uitgebreider onderzoek noodzakelijk is.

Het gaat dan allereerst om een verder verdiepend onderzoek naar de schade van ICT veiligheids- en betrouwbaarheidsproblemen. We bevelen aan een dergelijk onderzoek in nauwe samenwerking met alle relevante partijen op de Nederlandse ICT markt uit te voeren. Het commitment van deze partijen is van groot belang aangezien belangrijke delen van de benodigde informatie alleen voorhanden is bij deze partijen.

Ook een nader onderzoek naar de economische meerwaarde van vertrouwen in de veiligheid en betrouwbaarheid van de ICT-infrastructuur bij de eindgebruiker verdiepende inzichten geven. Wij denken dan bijvoorbeeld aan onderzoek naar de relatie tussen het gebruik van internet door consumenten en vertrouwen in ICT veiligheid en betrouwbaarheid en aan een verdere verdieping van de inschatting van de totale economische potentie en het economische risico van vertrouwen.

Bijlage I Geïnterviewde organisaties

	Organisatie
1.	NFIA
2.	Amsterdam in Business
3.	KPN
4.	Tele2
5.	ABN-Amro
6.	IBM
7.	Cisco
8.	Highmount Capital
9.	Nederlandse Vereniging van Banken
10.	Foreign Bankers Association (kort telefonisch)
11.	Nederlands Verbond van Verzekeraars
12.	Zorgverzekeraars Nederland
13.	Thuiswinkel.org
14.	ICT Office
15.	BTG
16.	Transport & Logistiek Nederland
17.	Nederlandse Vereniging van Groothandels
18	VNO-NCW/MKB-Nederland

Bijlage II Kwaliteitsaspecten van veilige en betrouwbare ICT-infrastructuur

Veilig en betrouwbaar datanetwerk

De *beschikbaarheid* van een datanetwerk bepaalt of er digitale gegevensuitwisseling kan plaatsvinden op een bepaald moment. De *(dis)continuïteit* van een datanetwerk bepaalt in welke mate deze onverstoord functioneert, zonder dat het netwerk tijdelijk buiten bedrijf is en geen gegevensuitwisseling kan plaatsvinden.

De *integriteit* van een datanetwerk bepaalt de kwaliteit van de digitale gegevensuitwisseling in termen van:

- Juistheid: worden gegevens uitgewisseld zonder dat deze tussen verzenden en ontvangen zijn gewijzigd?
- Volledigheid: ontbreken bij ontvangst gegevens die wel zijn verzonden?
- Tijdigheid: zijn gegevens op het moment van ontvangen nog actueel en bruikbaar?
- Controleerbaarheid: Is te achterhalen dat gegevens juist, volledig en tijdig zijn uitgewisseld?

De *exclusiviteit/vertrouwelijkheid* van een datanetwerk bepaalt welke gebruikers, informatiebronnen en internetdiensten gerechtigd zijn om toegang te krijgen tot het netwerk, zodat zij gegevens kunnen uitwisselen met andere gebruikers, informatiebronnen en internetdiensten.

Veilige en betrouwbare informatiebron

De *beschikbaarheid* van een database of informatiesysteem bepaalt of een gebruiker informatie kan opvragen of opslaan op een bepaald moment. De *(dis)continuïteit* van een informatiebron bepaalt in welke mate deze onverstoord functioneert, zonder dat deze tijdelijk buiten bedrijf is en geen informatielevering kan plaatsvinden.

De *integriteit* van een database of informatiesysteem bepaalt de betrouwbaarheid en veiligheid van het functioneren in termen van:

- Juistheid: Wordt de juistheid van de informatie die staat opgeslagen in de database of het informatiesysteem niet aangetast tijdens het verstrekken van de door de gebruiker opgevraagde informatie?
- Volledigheid: Wordt de informatie die wordt opgevraagd door de gebruiker in zijn volledigheid verstrekt zoals deze aanwezig is in de database of het informatiesysteem?
- Tijdigheid: Blijft de tijd die de database of het informatiesysteem nodig heeft om de informatie te verstrekken aan de gebruiker binnen van tevoren vastgelegde marges?
- Controleerbaarheid: Is de juistheid, volledigheid en tijdigheid van het functioneren van de database of het informatiesysteem te controleren?

De exclusiviteit van een database of informatiesysteem bepaalt welke gebruikers, informatiesystemen en internetdiensten gerechtigd zijn om toegang te krijgen tot een database of informatiesysteem om informatie op te vragen, te wijzigen en/of op te slaan.

In dit onderzoek richten wij ons niet primair op het vaststellen van de integriteitsaspecten van de informatie die databases of informatiesystemen beschikbaar stellen. Bijvoorbeeld de juistheid van gegevens in een database of informatiesysteem kan niet meer worden gezien als een aspect van ICT-infrastructuur, omdat de beheerder van die database of dat informatiesysteem, die rechtmatig toegang heeft, fouten kan maken die kunnen leiden tot onjuistheden in de informatiebron. Hiervoor zijn controles of veiligheidsmaatregelen in te richten, zoals goede voorlichting van medewerkers ter voorkoming van frauduleus gebruik van de informatie die zij omwille van hun beroepsmatige functie tot hun beschikking hebben. Het voorlichten van medewerkers is primair de verantwoordelijkheid van de organisatie die de database of het informatiesysteem beheert en niet de verantwoordelijkheid van de ICT-infrastructuur zoals gedefinieerd aan het begin van dit hoofdstuk. Deze maatregelen zijn echter dermate van belang voor de integriteit van de informatie die organisaties van externe partijen verkrijgen dat we deze wel meenemen in dit onderzoek. Daarbij speelt het Ministerie van Economische Zaken, Landbouw en Innovatie een rol in het verschaffen van voorlichting over ICT veiligheid, mede aan Nederlandse organisaties. Wel kijken we naar de integriteit van transacties tussen informatiebronnen van organisaties onderling en tussen organisaties en burgers of consumenten. Dit zijn transacties tussen twee of meer partijen via het internet, waarbij de betrokken partijen zich moeten identificeren en authenticeren. Tevens dient er een uitwisseling van informatie of waarde plaats te vinden van essentieel belang is voor de bedrijfsvoering van de betrokken organisaties alsmede de voor de betrokken burger / consument. Hierbij gaat het om organisaties (bedrijven of instellingen) die een belangrijke maatschappelijke rol spelen en waarvan een hoge mate van integriteit moet kunnen worden verwacht, zoals overheidsinstellingen en financiële instellingen.