Cyber Security Manifest

mei 2012

Deel 1: het Cyber Security Manifest

Aanleiding
Met de presentatie van de Nationale Cyber Security Strategie in februari 2011 staat cyber security nadrukkelijk op de (politieke) agenda. Incidenten in 2011 en 2012 benadrukken het belang voor deze integrale strategie voor cyber security. Met dit manifest beoogt ICT~Office richting te geven aan de verdere invulling van de Nationale Cyber Security Strategie en daarvoor een basis neer te leggen voor een visie en voor maatregelen die nodig zijn voor een *cyber secure* Nederland. Hierover wil ICT~Office het gesprek voeren met bedrijfsleven, met overheid, met de wetenschap.

Visie
Nederland is een hoogontwikkelde informatiesamenleving die voor de continuïteit van haar basisvoorzieningen en voor de economie sterk afhankelijk is van een adequaat werkende ICT-infrastructuur. De snel veranderende cyber security dreigingen vragen om een doortastende aanpak van zowel overheid als bedrijfsleven. Dit kan alleen als zij met internationale partners de handen ineenslaan op strategisch, tactisch en operationeel niveau.

Deze aanpak vereist dat kennis over en concrete ervaring met digitale veiligheid wordt samengebracht om de weerbaarheid van Nederland te waarborgen. Maatregelen zijn nodig waarmee flexibel, alert en krachtig kan worden gereageerd op nieuwe ontwikkelingen en dreigingen. Dit voorkomt vervelende verrassingen voor burgers en zorgt voor een veilige omgeving voor het (internationale) bedrijfsleven.

ICT~Office vindt het belangrijk dat de maatregelen worden genomen op (inter)nationaal niveau, organisatieniveau en individueel niveau.

Maatregelen op (inter)nationaal niveau
Op nationaal niveau is het belangrijk dat er een coherent raamwerk is waarin risico's op verstoring en maatregelen die de weerbaarheid vergroten zijn vastgelegd. Het is belangrijk dat maatregelen, inclusief regelgeving, passen binnen dit raamwerk. Principes als *privacy-by-design* en *secure-by-design* versterken de beveiliging van ICT-oplossing. De overheid dient deze te stimuleren en samen met de ICT-industrie op internationaal niveau in te vullen. Het is aan sectoren om concrete richtlijnen voor beveiliging op te stellen, de overheid heeft een rol dit te stimuleren. Van belang is dat positieve prikkels worden gecreëerd voor organisaties om hun beveiliging te vergroten en er op (inter)nationaal niveau de juiste randvoorwaarden zijn om te investeren in informatiebeveiliging.

Maatregelen op organisatieniveau
ICT is complex en divers. Een balans tussen effectief en werkbaar beveiligen in organisaties is essentieel. Voor passende beveiliging is het belangrijk dat organisaties weten wat hun huidige (on)veiligheid is en dat zij informatie en processen indelen naar beveiligingsniveaus. Een risicoanalyse op de organisatie en het implementeren van beveiligingsrichtlijnen vormen de basis hiervan. Beveiliging dient zich niet alleen te richten op de dreiging van buiten, maar ook op de risico's van binnen de organisatie. Organisaties dienen voor informatiebeveiliging standaard middelen te reserveren als percentage van het totale budget. Het is belangrijk dat in aanbestedingen beveiliging altijd meegenomen wordt.

Maatregelen op individueel niveau
De gebruiker is vaak de zwakste schakel. Bewustzijn is de voorwaarde voor beveiliging. Het management van een organisatie dient het voorbeeld te geven en in de organisatie aandacht te vragen hiervoor. Beveiliging heeft vooral zin als de eindgebruiker hiermee goed weet om te gaan.

Deltaplan cyber security
Deze maatregelen kunnen een plek te krijgen in een nationale aanpak voor cyber security op basis van samenhangende doelen. ICT~Office pleit voor een gemeenschappelijk deltaplan cyber security. In dit deltaplan dient de weerbaarheid in de vitale sectoren tegen verstoringen van ICT prioriteit te krijgen. Gebaseerd op de te beschermen belangen, de dreiging van deze belangen en het geaccepteerde risico in de digitale maatschappij, is een samenhangend raamwerk van maatregelen nodig waarin de juiste balans tussen preventie, detectie en respons is gevonden. Een gemeenschappelijk plan vraagt om betrokkenheid en inzet van belanghebbenden, waarin de rolverdeling tussen belanghebbenden helder wordt gedefinieerd.

Aspecten cyber security
De maatregelen die een plaats moeten krijgen voor een digitaal veiliger Nederland worden in de bijlage toegelicht onder de volgende verdeling:

A. Weerbaarheid tegen verstoring vergroten door te investeren in preventieve en proactieve maatregelen: door de veiligheid van ICT te versterken, bewustzijn als voorwaarde voor beveiliging te zien, de organisatie rondom ICT-beveiliging te verbeteren, preventieve maatregelen te vergroten en goed opdrachtgeverschap als basis te nemen
B. Actuele dreigingsinformatie monitoren, leren van incidenten stimuleren, positieve prikkels creëren en selectief zijn met nieuwe regelgeving
C. Fundamenten voor een veilige digitale wereld op orde brengen, zoals e-identiteit
D. Crisisorganisatie inrichten die helder en daadkrachtig is
E. Opsporing en vervolging laten aansluiten bij de praktijk

Alle belanghebbenden hebben een rol in cyber security
Om van de aanpak van cyber security een succes te maken is het belangrijk dat verschillende belanghebbenden hun bijdrage leveren. Hieronder heeft ICT~Office een eerste schets gemaakt van de rolverdeling.

Aan de Cyber Security Raad
› Stimuleer de ontwikkeling van een deltaplan cyber security, inclusief de benodigde 'dijkhoogte'.
› Controleer of er een coherent raamwerk is dat beschrijft welke cyber security maatregelen nodig zijn om Nederlandse belangen te beschermen tegen bekende en toekomstige dreigingen.
› Stuur aan op de ontwikkeling van betrouwbare digitale identificatiemiddelen.

Aan de overheid als regelgever en beleidsmaker
› Creëer vooral prikkels die organisaties stimuleren om vooraf beveiliging op orde te maken.
› Waarborg in regelgevende kaders de flexibiliteit om te reageren op nieuwe ontwikkelingen en zorg dat deze technologieneutraal en proportioneel zijn, zodat zij geen innovatie belemmeren.
› Stimuleer sectorspecifieke beveiligingsrichtlijnen, waarbij (internationale) normen en *best practices* de basis vormen.
› Versterk internationale publieke en private samenwerking voor het veiliger maken van ICT.
› Maak ICT een standaardvak op de middelbare school en maak beveiliging onderdeel daarvan
› Focus publiekscampagnes op burgers, ondernemers en vooral (top)management organisaties.
› Stimuleer het debat over de ordening van en controle op beveiliging van ICT-systemen, ondermeer over het versterken van en daadwerkelijk testen bij audits.

Aan het Nationaal Cyber Security Centrum

› Richt een meldpunt in waar organisaties vertrouwelijk incidenten kunnen melden en delen, zodat bedrijven en overheden van elkaar leren.
› Zet scenario's rond ICT-verstoring op die overheid en bedrijfsleven samen beoefenen.
› Zorg dat voor een continu zicht op de werkelijke cyberbedreigingen, creëer een voorspellende waarde voor nieuwe dreigingen en zorg voor ontsluiting hiervan naar overheid en bedrijfsleven.

Aan de ICT-branche

› Neem internationaal initiatief om beveiligingsniveaus van ICT-producten verder te verhogen.
› Geef voorlichting en adviseer klanten over de beveiliging van netwerken, systemen en data en de rol die de eindgebruiker heeft in de beveiliging
› Stimuleer principes als *privacy-by-design* en *secure-by-design*, ook in eigen producten.
› Werk samen met de auditsector aan snelle doorontwikkeling van eigentijdse en effectieve referentiekaders, normen en standaarden voor audits.

Aan de centrale en decentrale overheid als ICT-gebruiker

› Geef als overheid het goede voorbeeld in de beveiliging van informatiesystemen.
› Werk voor de kennis en (internationale) *best practices* over de informatiebeveiliging van het eigen ICT-landschap samen met de ICT-branche.
› Neem beveiliging adequaat en expliciet mee in elke opdracht en elke aanbesteding.

Aan organisaties als ICT-gebruiker, publiek en privaat

› Stel als organisaties in een vitale sector concretere richtlijnen op voor beveiliging.
› Heb inzicht in de samenstelling van het ICT-landschap en beveilig onderdelen bewust.
› Zorg voor een stevige basisbeveiliging van netwerk en data en voor monitoring om kwetsbaarheden en dreigingen snel te kunnen ontdekken. Test dit regelmatig.
› Beleg informatiebeveiliging in de organisatie transparant en creëer een sterker bewustzijn voor beveiliging in het gebruik van systemen maar ook voor het beheer (updaten) van de ICT.
› Neem adequate maatregelen voor een veilig gebruik van ICT in de organisatie en voor opleiding en training van personeel.

Aan de eindgebruiker

› Wees alert op nieuwe bedreigingen voor de beveiliging en volg adviezen van de organisatie op.
› Vraag om beveiligingstraining die voorkomt dat de eindgebruiker de zwakste schakel blijft.

Deel 2: Uitwerking Cyber Security Manifest

Risicomanagement als basis voor cyber security
Informatiebeveiliging is risicomanagement en dient daarom onderdeel te zijn van de totale risicobeheersing van een organisatie. Het gaat hierbij lang niet altijd om moedwillig misbruik, maar ook om onbedoeld falen van mensen en techniek. Een groot deel van de beveiligingsrisico's komt vanuit de eigen organisatie. Organisaties moeten daarom naast externe dreiging zicht hebben op deze dreigingen van binnenuit.

Beveiliging heeft aandacht nodig in de gehele keten van de ICT-infrastractuur, van document tot datacenter. Maatregelen voor beveiliging (techniek, organisatie en mensen) kunnen niet beperkt blijven tot één schakel.

Beveiliging en continuïteit dienen in iedere organisatie, management en project te zijn geïntegreerd met eindverantwoordelijkheid op het hoogste niveau. Een integrale benadering op de factoren mensen, processen en technologie is daarbij nodig. Belangrijk is dat middelen voor beveiliging standaard en zichtbaar worden gereserveerd in het budget voor ICT en projecten.

A. Weerbaarheid vergroten met preventieve en proactieve maatregelen

Veiligheid van producten en oplossingen versterken
Secure-by-design en *privacy-by-design* zijn fundamentele principes die de beveiliging van ICT-oplossingen versterken. Voor oplossingen op maat is het echter wel belangrijk dat wordt verduidelijkt wat onder de principes wordt verstaan. Voor ICT-producten dienen deze principes samen met de industrie op internationaal niveau te worden ingevuld.

Veelvoorkomende fouten in software leiden tot kwetsbaarheden. Daarom is het belangrijk software te testen op de meest voorkomende kwetsbaarheden. Bij de ontwikkeling van software en voor het testen kunnen bestaande overzichten, zoals die van OWASP of SANS CWE, als uitgangspunt worden genomen. De standaard PCI DSS (requirement 6) geeft een voorbeeld voor dit proces.

ICT is zeer complex en divers. Een balans tussen effectief beveiligen en werkbaar beveiligen is essentieel. Dit maakt het moeilijk om een standaard beveiligingsniveau te definiëren. De ICT-branche zal internationaal het initiatief moeten nemen om beveiligingsniveaus van producten verder te verhogen en nog alerter te reageren op nieuw bekend geworden dreigingen.

Overheden doen er goed aan om internationaal sterker samen te werken in de aanpak van veiligere ICT en niet slechts binnen hun eigen grenzen regels te ontwikkelen. De dreigingen zijn immers grotendeels internationaal. Op Europees niveau kan met de sector worden gewerkt aan een risico assessment. Hiervan bestaan reeds meerdere methodologieën. Een voorbeeld zou de *USA IT sector Baseline Risk Assessment* kunnen zijn.

ICT-bedrijven dienen hun expertise proactief in te zetten om de klant te adviseren over beveiliging van netwerken, systemen en gegevens en moeten zich bewust zijn van de rol die zijzelf hebben in de beveiliging van producten.

Bewustzijn als voorwaarde voor alle beveiliging
Zowel overheid als bedrijfsleven hebben een rol in het bewustwordingsproces van eindgebruikers. Zonder een duidelijk bewustzijn bij de mens kan veel worden geïnvesteerd in veilige producten en waarschuwingen maar hebben deze geen effect. Beveiliging en bewustzijn gaan samen.

Om bewustzijn vanaf de basis te bereiken, moeten aspecten van cyber security zijn geïntegreerd in alle niveaus in het reguliere onderwijs en in het bijzonder ook in het ICT-onderwijs. Ook hierom is het belangrijk dat ICT een standaardvak op de middelbare school wordt. *Secure-by-education* kan als nieuw fundamenteel principe het bewustzijn rond dreigingen vergroten. Onderwijsinitiatieven in de Verenigde Staten kunnen een voorbeeld zijn, bijvoorbeeld met het instellen van cyber security beurzen.

De zwakste schakel voor beveiliging is uiteindelijk veelal de mens. Zonder bewustzijn kan onveilig handelen niet worden aangepast. Ook vanuit het management is voldoende aandacht noodzakelijk. In de directiekamer is bewustzijn nodig over de waarden en belangen van de organisatie en de impact die (een verstoring van) ICT heeft.

Publiekscampagnes zijn belangrijk voor burgers en ondernemers. Gerichte campagnes zijn vooral nodig voor het (top)management van organisaties. Belangrijk is dat iedere organisatie met ondermeer interactieve tools en specifieke trainingen bewustzijn creëert bij zijn medewerkers.

Organisatie rondom ICT-beveiliging verbeteren
Het is belangrijk dat iedere organisatie, ook in het MKB, vaststelt wat zijn belangrijkste bedrijfsprocessen zijn, inzicht heeft in de informatie die de organisatie bezit of beheert en wat de belangrijkste bedreigingen zijn voor de bedrijfsprocessen of informatie.

Informatiebeveiliging dient in organisaties duidelijk en transparant belegd te zijn, met eindverantwoordelijkheid op het hoogste niveau.

Voorwaarde voor deze passende beveiliging is dat organisaties hun informatie en processen geclassificeerd hebben naar beveiligingsniveaus. Het is belangrijk dat organisaties weten hoe hun ICT-landschap en informatievoorziening eruit ziet, welke afhankelijkheden er zijn met de buitenwereld (en hoe zij worden geraakt als in de keten een schakel verdwijnt of onbetrouwbaar wordt) en op welke manier gegevens worden verwerkt.

Het internationale dataverkeer en de 'vitale' internetknooppunten vormen de *fundering* van het internet. Zorg dat de continuïteit daarvan goed is geborgd.

Preventieve maatregelen binnen de organisatie vergroten
Iedere organisatie dient een eigen beveiligingsbeleid te hebben, gericht op het beschermen van informatie en systemen en het verkleinen van de impact van een inbreuk of verstoring.

Het is belangrijk dat organisaties als basis van de beveiliging een veilig netwerk hebben, gevoelige data beschermen, in staat zijn kwetsbaarheden te ontdekken, een sterk toegangsbeleid hebben waarbij alleen diegene toegang hebben tot data die daartoe ook geautoriseerd zijn, en regelmatig de beveiliging testen.

Voor een snelle en adequate reactie op dreigingen is detectie een wezenlijk onderdeel. Real-time monitoring van belangrijke processen en systemen is van groot belang om passende acties te nemen bij actuele dreigingen en om van ontwikkelingen te leren voor continue verbetering.

Veel organisaties zijn kwetsbaar door het niet tijdig (kunnen) updaten van hun software. Het ongetest patchen vormt echter een risicofactor. Vanwege de soms complexe ICT-omgevingen is het nodig een update eerst te testen alvorens deze door te voeren. Een sterker bewustzijn voor het belang van patches en het leren van *best practices* dragen bij aan een beter patch-management.

Internationale normen, standaarden en *best practices* zijn beschikbaar voor het beveiligen van cruciale ICT-onderdelen. Eén normenkader is niet op te stellen. Een pragmatische aanpak is het wanneer sectoren met een gelijkend ICT-landschap in samenwerking met relevante leveranciers zelf concretere beveiligingsrichtlijnen opstellen en zichzelf aan deze richtlijnen houden.

Goed opdrachtgeverschap vormt basis voor goede beveiliging
Binnen publieke en private organisaties is beperkte kennis aanwezig om alle informatiebeveiliging van het ICT-landschap uit te voeren. Expertise van buiten de organisatie is hierbij onontbeerlijk, ook bij de overheid. Het is verstandig wanneer de overheid meer gebruik maakt van de kennis en van (internationale) *best practices* van het bedrijfsleven. Hieraan kan vorm worden gegeven in publiek-private samenwerkingsverbanden.

Goed opdrachtgeverschap is van cruciaal belang. In elke ICT-gerelateerde opdracht en aanbesteding dient beveiliging adequaat en expliciet te worden meegenomen, op basis van een vooraf uitgevoerde risicoanalyse of vastgestelde richtlijnen.

B. Monitor actuele dreigingsinformatie, stimuleer leren van incidenten, creëer positieve prikkels, wees selectief met nieuwe regelgeving

Het is belangrijk dat informatie over werkelijke cyberdreigingen (*threat intelligence*) continu door overheidsdiensten wordt verzameld en geanalyseerd. Uit deze monitoring volgt ook voorspellende informatie waardoor nieuwe dreigingen nog sneller voorzien en ondervangen kunnen worden. Deze kennis dient ook ontsloten te worden voor bedrijfsleven, zodat deze daarop kan anticiperen.

Organisaties kunnen veel van elkaars incidenten leren. Hiervoor is een meldingssystematiek nodig die het leren voorop stelt. Meldingen kunnen dan in vertrouwen worden gedeeld zonder risico op strafrechtelijke vervolging. Een voorbeeld kan hierbij worden genomen aan de luchtvaartsector, waar ook bijna-incidenten vertrouwd en zonder betrokkenheid van justitie worden gedeeld.

Een coherent raamwerk is nodig waarin risico's en de maatregelen zijn vastgelegd die de weerbaarheid tegen ICT-verstoring vergroten. Binnen de totale set aan maatregelen kan regelgeving een plaats krijgen, maar als sluitstuk op de brede aanpak. Veiligheid wordt niet gemaakt met alleen regels.

Sectoren kunnen door middel van zelfregulering sectorspecifieke beveiligingsrichtlijnen opstellen, waarbij (internationale) normen de basis vormen. Een voorbeeld is de concept *USA electricity subsector cyber security risk management process*. De overheid heeft een voorbeeldfunctie hierin om voorschriften op te stellen voor diensten van de e-overheid. Een coherent raamwerk voorkomt verzuiling in de cyber security aanpak tussen sectoren.

Als er sprake is van regelgeving en richtlijnen dan moeten deze technologieneutraal, beperkt en specifiek zijn voor het datgene waarvoor het is bedoeld, zodat deze geen innovatie belemmeren.

Creëer vooral prikkels die organisaties stimuleren om vooraf hun beveiliging op orde te maken (lagere premie verzekering, lagere boeteclausule) in plaats van negatieve prikkels (sancties) indien het verkeerd gaat. Een verregaande optie is het geven van fiscaal voordeel op security investeringen. Belonen motiveert, straffen frustreert.

Sancties zijn alleen effectief als er een eerlijke grondslag is en organisaties zelf in controle zijn voor het beperken van de impact. Over het algemeen verhogen sancties vooral de discussie over de aansprakelijkheid in plaats van de beveiliging.

C. Fundamenten voor een veilige digitale wereld op orde, zoals e-identiteit
Betrouwbare digitale identificatiemiddelen zijn nodig voor het doorontwikkelen en beveiligen van elektronische diensten, publiek en privaat. De overheid dient het initiatief voor deze e-identiteit te nemen. Niet alleen zal dit leiden tot een betrouwbaardere digitale communicatie tussen overheid, bedrijfsleven en burger en daarmee toenemende efficiency, ook is een e-identiteit zeer belangrijk voor het vertrouwen van burgers in de digitalisering van de samenleving.

Een debat is nodig over de ordening van en controle op de beveiliging van ICT-systemen. Zorg dat voor de inrichting ervan ook voorbeeld wordt genomen aan de fysieke wereld, bijvoorbeeld met voorbeelden uit de sector keren en beheren van oppervlaktewater. Hoe wordt bepaald welk risico aanvaardbaar is, welke dijkhoogte is daarvoor voldoende, hoe worden gebreken opgespoord en wat is de response bij (dreigende) doorbraak?

Controle en toezicht zijn een noodzakelijk onderdeel van informatiebeveiliging. De frequentie en diepgang van beveiligingsaudits moet zijn afgestemd op de benodigde betrouwbaarheid. Er kan meer gebruik worden gemaakt van geautomatiseerd auditing. Audits, inclusief het daadwerkelijke testen van systemen, zouden naast compliance gericht moeten zijn op onderdelen van het primaire proces, op basis van een risicoanalyse. Voor zeer kritische systemen zou een model van onaangekondigde audits kunnen gelden, op basis van 'high trust'. De gehele keten dient daarbij geaudit te worden, van opdrachtgevers tot opdrachtnemers.

D. Crisisorganisatie bij ICT-verstoring moet helder en daadkrachtig zijn
Ontwikkel standaardscenario's voor ICT-verstoringen en oefen deze scenario's periodiek samen met het bedrijfsleven, zowel op uitvoerings- als op beslissersniveau. Oefening helpt niet alleen om beter op elkaar in te spelen voor het geval van een crisis, ook draagt het bij aan bewustwording.

Een duidelijke crisisstructuur is nodig in geval van grootschalige ICT-verstoring. Zorg voor heldere verantwoordelijkheden en bevoegdheden om daadkrachtig op te kunnen treden bij een crisis. Hierbij moet ook de relatie tot het bedrijfsleven zijn geregeld. Samenwerking heeft de sterke voorkeur boven doorzettingsmacht.

Zorg dat de crisisorganisatie een duidelijk inzicht heeft in de responscapaciteit van partners en de juiste 'hulptroepen' ingezet kunnen worden. Maak daarvoor vooraf afspraken over de inzet van die capaciteit bij diverse incidentniveaus.

E. Opsporing en vervolging laten aansluiten bij de praktijk
Meer aandacht is nodig hoe organisaties om dienen te gaan met een digitale inbraak. Zorg voor een checklist voor organisaties, zodat zij weten hoe aangifte te doen en op welke manieren sporen veiliggesteld kunnen worden, maar ook hoe ze beste kunnen communiceren over het incident.

Er dienen goede, up-to-date strafrechtelijke kaders te zijn om cybercriminelen aan te pakken. Deze kaders hebben een mate van flexibiliteit nodig om te reageren op ontwikkelingen. Richt hierbij op degene die het vertrouwen in de digitale wereld ondermijnt.

Ethische hackers kunnen een nuttige bijdrage leveren in het opsporen van kwetsbaarheden en het testen van nieuwe ontwikkelingen. Ze tasten echter ook het vertrouwen in internetdiensten aan. Ethische hackers die zonder opdracht digitaal inbreken op systemen van derden kunnen niet vrij van vervolging blijven. Wanneer een ethische hacker een opgemerkte kwetsbaarheid zonder voordeel ervan te verkrijgen of schade aan te richten, dit meldt bij de organisatie die het betreft of een centraal meldpunt en zijn ontdekking vertrouwelijk houdt, kan vervolging achterwege blijven.

Cyber security bij ICT~Office

ICT~Office is de brancheverenigingvan meer dan 550 IT-, Telecom-, Internet- en Officebedrijven in Nederland. Met een achterban die dertig miljard euro omzet en 250.000 medewerkers telt, is ICT~Office dé belangenbehartiger en vertegenwoordiger van de Nederlandse ICT-branche.

De betrokkenheid van ICT~Office bij cyber security is groot. Voor een veilige en vertrouwde inzet en gebruik van ICT is digitale veiligheid (cyber security) en continuïteit van ICT van cruciaal belang, zowel in een publieke als private omgeving. De Nederlandse ICT-branche is als leverancier van ICT-infrastructuur, -producten en -diensten een natuurlijk partner op het gebied van cyber security. ICT~Office wil in die rol bijdragen aan het vergroten van de digitale veiligheid van Nederland.

ICT-branche betrouwbaar en deskundig partner op cyber security
Publiek-private samenwerking is van groot belang om de versterking van cyber security tot een succes te maken. ICT~Office streeft ernaar een betrouwbaar en deskundig partner te zijn op cyber security, ondermeer door het voortouw te nemen in deze samenwerking. Als lid van de Cyber Security Raad levert ICT~Office een actieve bijdrage in het verstevigen van de cyber security agenda in Nederland. Daarvoor werkt ICT~Office samen met partners uit overheid, bedrijfsleven en wetenschap. Ook werkt ICT~Office nauw samen met het Nationaal Cyber Security Centrum.

In de samenwerking met het CIO Platform wil ICT~Office de dialoog bevorderen tussen ICT-leveranciers en grote ICT-gebruikers over de vraagstukken rond cyber security. Daarnaast werkt ICT~Office samen met het programma Digiveilig bij ECP om de kennis en expertise van de ICT-branche in te zetten voor een sterker beveiligingsbewustzijn bij gebruikers. Via de website www.beschermuwonderneming.nl biedt ICT~Office daarvoor al enkele handvatten.

Adviesgroep cyber security
Het *Cyber Security Manifest* is geïnitieerd door de adviesgroep cyber security van ICT~Office en is mede tot stand gekomen met kennis en bijdrages van de deelnemende lidbedrijven in de adviesgroep cyber security en de expertgroep informatiebeveiliging.

De adviesgroep cyber security signaleert de voor de ICT-branche relevante ontwikkelingen wat betreft cyber security en adviseert het bestuur van ICT~Office over standpunten en activiteiten. Daarbij bespreekt de adviesgroep ook de inbreng van ICT~Office in de Cyber Security Raad. Leden van deze adviesgroep zijn vertegenwoordigers van ICT-bedrijven aangesloten bij ICT~Office die, op strategisch niveau binnen de organisatie, eindverantwoordelijk zijn voor cyber security.

Expertgroep informatiebeveiliging
De expertgroep Informatiebeveiliging binnen ICT~Office biedt lidbedrijven de ruimte om te klankborden op en hun expertise in te zetten voor het onderwerp informatiebeveiliging en de vergroting van het bewustzijn daarvan.