Het kielzog van de websurfer

Ir. R. de Wolf RE

Het internet wordt door beveiligingsexperts vaak geschetst als een anarchistische digitale wereld, waarin de 'netburgers' een anoniem en ontraceerbaar leven leiden. Het lijkt daarom wel goed te zitten met de privacy van de netburger. Niets is echter minder waar. De belangrijkste show-stopper voor zakelijke internettoepassingen is dan ook het gebrek aan vertrouwen bij netburgers in beveiliging en privacy op het internet.

Inleiding

In de technische infrastructuur van het internet ontbreken allerlei belangrijke bouwstenen voor de bescherming tegen diefstal van informatie. Informatie kan tijdens het transport over het internet door afluisterpraktijken of als gevolg van computerinbraken in verkeerde handen vallen. Dit geldt ook voor vertrouwelijke of persoonlijke informatie over netburgers. Ook laat de netburger tijdens het surfen op het web bewust en onbewust veel sporen na over bijvoorbeeld het persoonlijk leven, interessegebieden en toekomstige aankopen. Meerdere onderzoeken wezen uit dat de bezorgdheid over privacy en de beveiliging van vertrouwelijke informatie veel netburgers ervan weerhoudt om via het internet zaken te doen[1].

Bij de Nederlandse (net)burgers kan een deel van deze bezorgdheid door de komst van de nieuwe Wet bescherming persoonsgegevens (Wbp)[2] worden weggenomen. Deze wet- en regelgeving op het gebied van privacybescherming legt het aanleggen en bewerken van gegevens over individuele personen, dus ook via het internet, sterk aan banden. Daarnaast biedt de Wbp meer rechten en zekerheden ten aanzien van de controle op en de beveiliging van gegevens die over hen zijn vastgelegd.

In dit artikel wordt ingegaan op de impact van de inwerkingtreding van de Wbp op het internet. In het eerste deel worden na een korte schets van de kernpunten van de Wbp enkele thema's behandeld die de discussies rond privacy op het internet domineren. Ook wordt kort stilgestaan bij de technische mogelijkheden om gegevens te verzamelen over het surfgedrag van netburgers en hoe dit is tegen te gaan.
In het tweede deel van het artikel wordt ingegaan op de gevolgen van de inwerkingtreding van de Wbp voor de aanbieders van internetdiensten en in het bijzonder welke privacybeschermende maatregelen op basis van de Wbp voor websites dienen te worden getroffen. Ten slotte wordt aandacht besteed aan de rol van de IT-auditor bij de toetsing op de naleving van de privacywetgeving.

Wbp in het kort

Zoals in voorafgaande artikelen in deze Compact al uitgebreid is besproken, is per 1 september 2001 de Wet bescherming persoonsgegevens van kracht geworden. De Wbp is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en de handmatige verwerking in een zogeheten gestructureerd bestand. Persoonsgegevens zijn gegevens die een persoon direct of indirect uniek identificeren. De wet maakt onderscheid tussen *betrokkene* (van wie persoonsgegevens worden vastgelegd), *verantwoordelijke* (opdrachtgever van verzamelen en/of bewerken van persoonsgegevens), *bewerker* (onderaannemer die gegevens verzamelt of verwerkt) en *toezichthouder* (nu College Bescherming Persoonsgegevens geheten). De betrokkene heeft onder de Wbp het recht tot inzage van over hem of haar vastgelegde gegevens, het recht op correctie van deze gegevens en het recht op verzet. In het laatste geval kan de verantwoordelijke verplicht worden de gegevens te verwijderen. De verantwoordelijke heeft de plicht persoonsregistraties aan te melden bij het College of een daarvoor aangewezen functionaris binnen de organisatie of branche. Hierbij dient een duidelijk doel te worden aangegeven waarvoor de registratie wordt of is aangelegd. Bestaande registraties dienen voor 1 september 2002 te zijn aangemeld. Ook heeft de verantwoordelijke de plicht de betrokkene te informeren over de registratie en verdere verwerking, tenzij de betrokkene eerder hiervoor expliciet toestemming heeft gegeven, en binnen vier weken te reageren op verzoeken tot inzage en correctie. De verantwoordelijke en de bewerker hebben tevens een geheimhoudingsplicht ten aanzien van de verzamelde en/of bewerkte gegevens en dienen deze gegevens op adequate wijze te beveiligen. De verantwoordelijke en de bewerker mogen de persoonsgegevens alleen bewaren indien dit voor het beoogde doel noodzakelijk is. Ten slotte is onder de Wbp de registratie van bijzondere persoonsgegevens zoals godsdienst, levensovertuiging, ras of politieke gezindheid in principe verboden.

Het College stuurt als toezichthouder aan op zelfregulering. Hierdoor mag een verantwoordelijke zelfstandig of op brancheniveau een gedragscode tot stand brengen. Het College kan ook sancties opleggen. De belangrijkste daarvan is het uitoefenen van zogeheten bestuursdwang, waardoor het College een organisatie kan opleggen iets te doen of na te laten op straffe van een door hem te bepalen dwangsom. De hoogte van die dwangsom is niet aan een maximum gebonden.

Internet en privacythema's

U kent vast de briefkaarten die bij aankoop van bijvoorbeeld een stereotoren of huishoudelijk apparaat naar de fabrikant of distributeur moeten worden teruggestuurd. Deze kaarten geven weliswaar recht op garantie, maar in werkelijkheid zijn ze een weinig effectief instrument van fabrikanten om gegevens te verzamelen over de uiteindelijke kopers van deze producten. De meeste van deze kaarten gaan met de handleiding voorgoed in de kast of direct met de verpakking bij het grofvuil.

Tegenwoordig vult wel iedere netburger maar al te graag op de website van dezelfde fabrikant zijn of haar naam, adres, woonplaats en e-mailadres in om een handleiding, support of add-ons bij een pas gekocht product te kunnen ontvangen. Hierbij wordt vaak het kleine vinkje over het hoofd gezien waarmee de netburger ook instemt met het ontvangen van brochures of e-mailtjes over producten. Met hetzelfde enthousiasme ruilt de netburger zijn of haar gegevens ook in voor gratis internettoegang, e-maildiensten of software.

Het laagdrempelige, interactieve karakter van het internet is voor bedrijven en instellingen een zeer geschikt medium gebleken om gegevens te verzamelen over de klantenkring of doelgroep. Behalve naar e-mailadressen en NAW-gegevens wordt vaak ook gevraagd naar het type thuiscomputer, de naam van de werkgever en de functie bij die werkgever.

Naast het in bescherming nemen van de netburger tegen het vrijwillig verstrekken van persoonsgegevens, legt de Wbp ook beperkingen op aan het gebruik van technieken waarmee op het internet gegevens over netburgers kunnen worden verzameld, zonder dat deze hier weet van hebben. De belangrijke thema's die in publicaties over privacy op het internet steeds terugkeren, zijn dan ook spamming, privacyaspecten van internetgebruik op het werk, hacking en afluisterpraktijken. In het vervolg van deze paragraaf wordt kort ingegaan op de raakvlakken van de Wbp en de andere relevante wet- en regelgeving in Nederland met deze thema's.

Spamming

Elke netburger ontvangt regelmatig junk-mail. Mogelijk heeft hij eerder hiermee ingestemd bij het invullen van een formulier op een website. Het merendeel van deze junk-mail is echter het werk van zogeheten *spammers*. Spammers zijn personen of organisaties die op zeer grote schaal e-mailberichten aan netburgers versturen, zonder hiervoor vooraf om toestemming te vragen. De meer legitieme spammers bieden achteraf nog de mogelijkheid van de adressenlijst verwijderd te worden. Het hardnekkigste soort spammers stuurt echter een fictief afzenderadres mee, waardoor geen mogelijkheid bestaat te reageren, laat staan bezwaar te maken.

Hoe komen spammers aan e-mailadressen? En welke gegevens kunnen ze naast e-mailadressen nog meer over hun doelgroep hebben verzameld? De meest voor de hand liggende bron van e-mailadressen is het internet zelf. Spammers gebruiken bijvoorbeeld de adresboeken van gratis e-mailproviders en de afzenderadressen uit Usenet-nieuwsberichten. Ook worden e-mailadressen gebruikt als gebruikersnaam op internetveilingen zoals Ebay, waardoor ze vrij toegankelijk zijn. Spammers zijn vaak niet geïnteresseerd in andere informatie dan e-mailadressen. Het hoofddoel van spamming is niet zozeer zorgvuldig een band op te bouwen met potentiële klanten, maar een commerciële boodschap uit te dragen aan een zo groot mogelijke schare mensen. Hierbij wordt bewust het risico gelopen dat 99,9 procent van de ontvangers de boodschap direct naar de trashcan sleept.

Een e-mailadres op het internet is uniek. Als gevolg van afspraken in de onderliggende standaardprotocollen dient op het internet sprake te zijn van een eenduidige adressering van systemen, websites en brievenbussen. Dit wil niet zeggen dat een e-mailadres ook uniek identificerend is voor een persoon. E-mailadressen kunnen namelijk bestaan uit cijfercodes, initialen en pseudoniemen, waardoor geen directe relatie hoeft te bestaan met de naam van de eigenaar van het adres.

Spamming kan daarom niet altijd op basis van de Wbp worden aangepakt. De DMSA (een Nederlandse brancheorganisatie voor direct marketing) heeft als gevolg van de inwerkingtreding van de Wbp een gedragscode opgesteld om spamming door haar leden tegen te gaan. Deze 'Code Verspreiding Ongevraagde Reclame via e-mail' stelt dat e-mailberichten mogen worden verstuurd, tenzij de geadresseerde daar (vooraf of achteraf) bezwaar tegen maakt. Dit zogeheten 'opt-out'-systeem zal op termijn op grond van nieuwe Europese privacyrichtlijnen worden vervangen door een 'opt-in'-systeem, waarbij de ontvanger vooraf expliciet toestemming dient te geven voor het ontvangen van reclamemail[3].

Zolang e-mailberichten nog volledig anoniem via het internet kunnen worden verstuurd, zijn gedragscodes en privacywetten weinig effectieve maatregelen om de overlast als gevolg van spamming te verminderen.

Internetgebruik op het werk

De nieuwe privacywetgeving heeft ook gevolgen voor het recht op privacy van werknemers[3]. In de Wbp zijn de mogelijkheden die de werkgever heeft om zijn werknemers te controleren aan meer voorwaarden gebonden dan voorheen. In het bijzonder het controleren van het e-mail- en surfgedrag op het internet van werknemers heeft in een aantal recente gevallen tot het ontslag van werknemers geleid.

Als gevolg van deze zaken heeft de Registratiekamer geoordeeld dat bedrijven een gedragscode moeten vastleggen, waarin de regels rondom internetgebruik zijn opgenomen. De Registratiekamer heeft tevens een rapport gepubliceerd 'Goed werken in netwerken'[4] waarin wordt geconcludeerd dat controle mogelijk moet zijn, maar onder strikte voorwaarden. Zo moet de werkgever heldere afspraken over e-mail en internetgebruik maken met de ondernemingsraad en de werknemers. Deze afspraken moeten aan alle werknemers kenbaar worden gemaakt. Dit kan bijvoorbeeld door een gerichte boodschap op het openingsscherm van de webbrowser of het e-mailprogramma. De werkgever dient verder technische maatregelen te treffen om het ongewenste internetgedrag aan banden te leggen. Hierbij kan gedacht worden aan het blokkeren van websites die geen zakelijk doel hebben.

Hacking

Niet alleen spammers en werkgevers kunnen het privacygevoel op het internet geweld aan doen. Hackers die als sport of broodwinning via het internet computerinbraken plegen, hebben doorgaans weinig respect voor de persoonlijke levenssfeer van de netburger. Er zijn geslaagde computerinbraken bekend waarbij bijvoor-

beeld creditcardgegevens (www.cduniverse.com), bankafschriften (www.creditsuisse.com), belastinggegevens (www.hrblock.com) en medische gegevens (www.washington.edu/medical) zijn buitgemaakt. In juli dit jaar zijn door een hacker de persoonsgegevens van tweeduizend panelleden van het Nederlandse onderzoeksbureau Multiscope buitgemaakt. Ook raakte www.attrition.org, de bekende database van gekraakte websites of *defacements*, door de sterke toename van het aantal computerinbraken via websites in maart 2001 zo overvol, dat Attrition besloot te stoppen met het toevoegen van nieuwe defacements.

De netburger levert zijn of haar gegevens maar al te graag in voor gratis diensten.

De Wbp stelt in artikel 13 eisen aan de beveiliging van persoonsgegevens: 'De verantwoordelijke dient passende technische en organisatorische maatregelen te treffen om het verlies van gegevens of onrechtmatige verwerking ervan tegen te gaan. Deze maatregelen moeten een passend beveiligingsniveau garanderen, rekening houdend met de stand van de techniek en de kosten van de maatregelen. De maatregelen moeten er mede op gericht zijn onnodige verzameling of verdere verwerking te voorkomen.' De beveiliging moet dus voortdurend op niveau zijn, rekening houdend met technologische ontwikkelingen.

Dit houdt voor een website op het internet in dat op continue basis moet worden gecontroleerd of nieuwe beveiligingslekken zijn ontdekt die een negatieve weerslag kunnen hebben op de beveiliging van de site. De beheerders van websites hebben door het grote aantal publicaties van kwetsbaarheden vaak onvoldoende actuele beveiligingskennis om aan deze eis te voldoen. Het is daarom van belang periodiek de beveiliging van websites te laten controleren door onafhankelijke beveiligingsspecialisten.

Afluisterpraktijken

Als hackers een computersysteem hebben overmeesterd, zijn ze in principe in staat al het e-mailverkeer dat via dit systeem wordt geleid te onderscheppen. Ook kunnen alle toetsaanslagen op het systeem worden geregistreerd, waaronder wachtwoorden van legitieme gebruikers van het gekraakte systeem en alle andere systemen waarmee het gekraakte systeem relaties heeft. Dergelijke afluisterpraktijken behoren tot de technieken die hackers in staat stellen eenvoudig een reeks aan elkaar gerelateerde systemen te kraken.

Het afluisteren van internetverkeer kent echter ook legitieme doelen. De afgelopen jaren zijn door diverse kamerleden vragen aan de regering gesteld over het bestaan van het Amerikaanse afluistersysteem Echelon. Begin dit jaar is zelfs een hoorzitting van de vaste commissie voor inlichtingen en veiligheidsdiensten van de Tweede Kamer aan het onderwerp gewijd. Echelon zou zich echter niet alleen beperken tot internetverkeer, maar ook gericht zijn op het aftappen van nationale en internationale telefoonverbindingen, dataverbindingen, GSM-, SMS-, telex- en faxverkeer. Dergelijke systemen bestaan al vele jaren en dreigen door de extreme groei van het gebruik van telecommunicatiemiddelen ten onder te gaan aan de zogeheten 'intelligence overload'. Deze intelligence overload is een reden waarom de 'gewone burger' zich niet in zijn privacy aangetast hoeft te voelen, aldus een deskundige[5].

In Nederland is het aftappen van telecommunicatieverkeer opgenomen in de Telecommunicatiewet en het Wetboek van Strafvordering[6]. Het kernpunt van deze wetgeving is de medewerkingsverplichting die aan de telecommunicatiebedrijven wordt opgelegd. De telecommunicatiesignalen worden op basis van een bevoegd gegeven last of bevel in opdracht van de bevoegde autoriteit door de telecommunicatiebedrijven op een gerichte wijze getapt. Deze bevoegde autoriteiten zijn opsporingsdiensten zoals de politiediensten, het CRI en de FIOD. Voor de Binnenlandse Veiligheidsdienst (BVD) en de Militaire Inlichtingendienst (MID) zijn de aftapbevoegdheden vastgelegd in het Wetboek van Strafrecht en in het wetsvoorstel tot herziening van de Wet op de inlichtingen- en veiligheidsdiensten (wetsvoorstel Wiv).

Bij deze vormen van afluisterpraktijken weegt het opsporings- respectievelijk het staatsveiligheidsbelang zwaarder dan het privacybelang van de burger en diens recht op een ongestoorde communicatie[7], zodat de impact van de Wbp op deze vorm van afluisterpraktijken beperkt zal zijn.

Het kielzog van de websurfer

In deze paragraaf wordt ingegaan op de sporen die rondsurfende netburgers op het web achterlaten, zonder dat zij zich hiervan bewust zijn. Ook wordt ingegaan op enkele privacyverhogende maatregelen die getroffen kunnen worden om het verzamelen van deze sporen door websites en zoekmachines tegen te gaan.

Cookies, Redirection, Javascripts en zoekmachines

Tijdens het raadplegen van websites en zoekmachines op het internet kunnen via een reeks verschillende technieken gegevens over de websurfer worden vastgelegd. De verreweg bekendste techniek baseert zich op zogeheten cookies. Cookies zijn kleine stukjes informatie die op initiatief van de bezochte website op de schijf van de websurfer worden opgeslagen. Een cookie bevat over het algemeen een uniek identificatienummer, zodat op basis van dit nummer de websurfer gedurende meerdere bezoeken kan worden getraceerd. De browser kan zo worden geconfigureerd dat hij geen cookies accepteert of alleen nadat hiervoor per cookie expliciet toestemming is gegeven. Als cookies via de browser zijn uitgeschakeld, kunnen via zogeheten HTML embedded cookies alsnog identificatienummers van de ene pagina naar de andere worden doorgegeven. Deze laatste vorm van cookies wordt echter niet op de harde schijf vastgelegd, waardoor deze cookies na afloop van het bezoek aan de site worden verwijderd. Hierdoor kan alleen gedurende het bezoek een profiel van de bezoeker worden samenge-

steld. Voor het tegengaan van het gebruik van HTML embedded cookies is nog geen oplossing gevonden.

Websurfers zoeken vrijwel altijd via een zoekmachine naar voor hen relevante informatie. De websurfer verraadt echter via de opgegeven trefwoorden zijn persoonlijke en zakelijke interesses. De trefwoorden van zoekmachines bieden door het met elkaar in verband brengen van zoektermen de mogelijkheid gedetailleerde profielen aan te leggen, zonder dat de websurfer zich hiervan bewust is[8]. Veel zoekmachines geven de zoektermen door aan adverteerders, zodat het niet verwonderlijk is dat de reclame-uitingen in de zoekmachine zich aanpassen aan de ingegeven zoektermen. Volgens een recent onderzoek naar privacyaspecten van zoekmachines lijken Google en Lycos de privacy van de websurfer nog enigszins te respecteren[9].

Niet alleen de zoektermen maar ook de keuze uit de zoekresultaten kunnen door zoekmachines worden vastgelegd. Als de websurfer op één van de treffers in de lijst van zoekresultaten klikt, komt hij niet direct op de gewenste site, maar wordt hij via de zoekmachine naar de site *geredirect*. Hierdoor kan de zoekmachine de gekozen zoekresultaten registreren en in verband brengen met bijvoorbeeld het identificatienummer van de websurfer in een cookie.

Als Javascript in de browser is geactiveerd, kunnen door de webserver tevens enkele configuratie-instellingen van de browser worden opgevraagd. Zo kunnen websites onder meer het type en versienummer van de browser, de taal van het besturingssysteem en de beeldscherminstellingen achterhalen.

Cookiemanagers, proxies, anonymizers en P3P

De meeste browsers stellen de websurfer in staat cookies en Javascript te deactiveren. Ondanks de privacyverhogende werking laten de meeste websurfers deze opties geactiveerd omdat anders de functionaliteit van websites te zeer wordt beperkt. Als alternatief kan voor cookies gebruikgemaakt worden van zogeheten cookiemanagers, waarmee selectief cookies van het systeem kunnen worden geweerd, dan wel achteraf kunnen worden verwijderd. Deze cookiemanagers zijn vaak public domain programma's en dus vrij op het internet te verkrijgen.

De websurfer kan ook via een proxy-server of anonymizer sites en zoekmachines op het internet raadplegen. Veel van de bovengenoemde technieken zijn dan niet meer effectief. Een proxy-server fungeert als doorgeefluik van webverkeer en dient bijvoorbeeld om informatie over de interne structuur van netwerken af te schermen van het internet, om het browsegedrag van werknemers in kaart te brengen of om door een caching-mechanisme de surfsnelheid te vergroten. Tevens kunnen proxy-servers op een aantal in de vorige paragraaf genoemde technieken filteren. Web anonymizers zijn proxy-servers die enkel tot doel hebben de privacy van de websurfer te beschermen. Naast het fysiek en logisch ontkoppelen van de surfer en het surfgedrag zijn web anonymizers in staat te filteren op cookies, applets en Javascript-toepassingen. In referentie 10 is een overzicht opgenomen van enkele web anonymizers.

De nieuwe browser van Microsoft, Internet Explorer 6 (IE6) bevat een implementatie van het P3P-protocol[11]. Dit protocol ondersteunt een aantal aanvullende mogelijkheden om de privacy van de websurfer te beschermen. Zo bevat IE6 vijf niveaus van cookie control. Op het laagste niveau worden alle cookies geaccepteerd en op het hoogste niveau worden alle cookies geweigerd. Het middelste niveau (defaultwaarde) accepteert alleen cookies met een zogeheten privacy policy. In dat geval kunnen gebruikers een 'opt-out'-optie tegen datacollectie benutten. Cookies zonder een dergelijke privacy policy worden geblokkeerd. Er wordt echter gevreesd voor het succes van deze feature, omdat het onderliggende P3P-protocol bij elk ontvangen cookie de bijbehorende XML-gebaseerde privacy policy zal opvragen bij de betreffende website. Dit kan de overhead van het webverkeer sterk doen toenemen. Microsoft hecht echter een verkorte versie van de policy aan de cookie, zodat verwerking on-the-fly mogelijk wordt. Nu voldoen nog maar enkele tientallen sites aan de Microsoft-variant van de P3P-standaard[12].

Impact Wbp voor aanbieders van websites

De aanbieders van websites waarbij persoonsgegevens worden verzameld of bewerkt, dienen zich bewust te zijn van de gevolgen van de Wbp. De wet en de toelichtingen hierop gaan niet expliciet in op de beveiliging van websites, maar er wordt op basis van artikel 13 geëist dat sprake is van een voldoende hoog beveiligingsniveau. In deze paragraaf wordt een vertaalslag gemaakt van de eisen in de Wbp naar de te treffen maatregelen voor websites op het internet.

> Op basis van artikel 13 van de Wbp wordt een voldoende hoog niveau van beveiliging van websites geëist.

Toepassingsgebied
Voor de aanbieders van websites heeft de verruiming van het toepassingsgebied van de Wbp belangrijke gevolgen. De Wbp is namelijk, in tegenstelling tot de Wpr, ook van toepassing op het verzamelen van gegevens, waarbij door de Wbp een sterke doelbinding wordt geëist. Dit heeft een grote impact op aanbieders van websites die pagina's bevatten waarmee gegevens worden gevraagd aan, dan wel worden verzameld over bezoekers van de sites. Tevens zijn in de Wbp richtlijnen opgenomen voor zowel de aanbieders van websites als alle bij deze site betrokken service providers. Voorbeelden van deze service providers zijn de Internet Service Providers (ISP's) die de toegang tot het internet en eventueel de hosting van websites verzorgen en Application Service Providers (ASP's) die zowel ISP-diensten als de hosting van de achterliggende informatiesystemen voor hun rekening nemen.

Melding
De registratie van persoonsgegevens van Nederlandse (net)burgers dient te worden gemeld aan het College Bescherming Persoonsgegevens. In het geval van het ver-

zamelen van persoonsgegevens via een website dient deze melding plaats te vinden door de eigenaar van de website. Het College heeft met ingang van 15 augustus 2001 een interactieve checklist op zijn website geplaatst, samen met een meldingsprogramma om de melding te automatiseren. Deze meldingsplicht geldt in elk geval voor de persoonsregistraties die al onder de Wpr waren gemeld. Nieuwe meldingen moeten worden ingediend voordat daadwerkelijk wordt aangevangen met de registratie of bewerking van persoonsgegevens. Belangrijk bij de melding is een nauwkeurige omschrijving van het doel van de registratie dan wel de bewerking van de persoonsgegevens.

Toestemming
De bezoeker van de site, ofwel de betrokkene in Wbp-jargon, moet toestemming geven voor het registreren van zijn of haar gegevens. Een vinkje plaatsen of een knop indrukken op een webpagina kan voldoende zijn, mits de betrokkene eerst voldoende over zijn of haar rechten wordt geïnformeerd. In de praktijk dient de betrokkene dus langs het privacystatement van de aanbieder te worden geleid voordat deze de registratie mag bevestigen. Op Amerikaanse sites wordt deze werkwijze al geruime tijd gevolgd voor software licence agreements en terms of use agreements voor bijvoorbeeld te downloaden programmatuur en gratis e-maildiensten.

Privacystatement
De aanbieder van een website dient het privacystatement duidelijk waarneembaar op de site te plaatsen. Dit privacystatement dient in te gaan op het beoogde gebruik van de gegevens, de wijze waarop de betrokkene bezwaar kan maken tegen het beoogde gebruik en eventueel de wijze waarop aan de betrokkene kenbaar zal worden gemaakt dat zijn of haar gegevens voor nieuwe doeleinden zullen worden gebruikt. Zo dient de dienstenaanbieder bij regelmatige verstrekking van de gegevens aan derde partijen de betrokkene minstens eenmaal per jaar hiervan op de hoogte te stellen (art. 41 Wbp). Tevens dient het statement in te gaan op de wijze waarop de bezoeker een verzoek tot inzage in de gegevens of een correctieverzoek kan indienen.

Geheimhouding
Zowel de aanbieder van de website als de betrokken service providers zijn onder de Wbp gehouden aan een geheimhoudingsplicht ten aanzien van de verzamelde persoonsgegevens. Hiertoe dient in contracten met service providers een passende geheimhoudingsclausule te worden opgenomen. Daarnaast dienen medewerkers van de aanbieder van de website die in aanraking komen met de persoonsgegevens een geheimhoudingsverklaring te tekenen.

Systeembeveiliging
Artikel 13 van de Wbp eist dat de eigenaar van de website passende technische en organisatorische maatregelen neemt om het verlies van gegevens of onrechtmatige verwerking tegen te gaan. Deze eisen laten zich voor het aanbieden van websites vertalen in de volgende categorieën beveiligingsmaatregelen:
* Het betrekken van beveiligingsaspecten in het ontwerp van de website. Een belangrijk aspect van systeembeveiliging in het kader van de Wbp is de identificatie van de bezoekers. Is degene die persoonsgegevens aanlevert of wijzigt wel wie hij zegt te zijn?
* Het treffen van best-practice beveiligingsmaatregelen ten aanzien van websiteontwikkeling en -beheer en de inrichting van technische bouwblokken waaruit de website is opgebouwd. Daarnaast dienen de de-factobeveiligingsmaatregelen voor het internet te worden getroffen, zoals firewalls en intrusion detection systemen. Deze systemen dienen om ongeautoriseerde toegang vanaf het internet tegen te gaan en inbraakpogingen snel te signaleren.
* Het waarborgen van de integriteit en vertrouwelijkheid van persoonsgegevens tijdens transport en opslag. De handleiding van het Ministerie van Justitie[13] noemt hierbij encryptie als mogelijke maatregel. Dit laat zich vertalen in de inzet van SSL-versleuteling op webpagina's waar de bezoeker om persoonsgegevens wordt gevraagd. Tevens kan de integriteit en vertrouwelijkheid van opgeslagen persoonsgegevens worden gewaarborgd door het toepassen van data-encryptie.

Internationaal internetverkeer
Websites met een Nederlandse top-level domeinnaam (eindigend op .nl) hoeven zich niet in Nederland te bevinden. Het is niet ongebruikelijk dat een Nederlandse organisatie haar website heeft ondergebracht bij een buitenlandse service provider. Indien met een in het buitenland ondergebrachte site persoonsgegevens van Nederlandse burgers worden verzameld, worden deze gegevens feitelijk geëxporteerd. De Wbp geldt echter ook voor dergelijke websites die buiten de Europese Unie worden gehost of voor persoonsgegevens die in opdracht van de aanbieder van de site buiten de EU worden verwerkt. Buitenlandse bedrijven die Nederlandse persoonsgegevens verzamelen of bewerken, moeten een persoon of instelling in Nederland als waarnemer aanwijzen, die de melding verzorgt en als contactpersoon fungeert voor het College. Het betreffende land moet echter een passend beschermingsniveau waarborgen en een vergelijkbare privacywetgeving hebben, anders is de uitvoer van persoonsgegevens niet toegestaan.

Praktijkvoorbeelden impact van de Wbp voor internetdiensten

Privacystatement bij aanmelding voor gratis internettoegang
Internet Service Providers die gratis internettoegang bieden, hebben vaak een on line aanmeldingsprocedure waarin de gegevens van de aanvrager worden vastgelegd en het e-mailadres, de gebruikersnaam en de toegangscode van de aanvrager worden bepaald. Dit geldt ook voor Wanadoo, waar tijdens de aanmeldingsprocedure expliciet dient te worden ingestemd met de voorwaarden, waaronder in artikel 10 de richtlijnen omtrent privacy en gegevensbescherming. Hierin komen zaken aan bod als de melding aan het College, de doelbinding, de bewaartijd na beëindiging van het abonnement, systeembeveiliging en het recht tot inzage en correctie.

Restricties op de directory services van Surfnet
Als gevolg van de Wbp mogen de directory services van SurfNet met gegevens over individuele personen, zoals LDAP- en WHOIS-databases, niet seriematig

bevraagbaar zijn zodat kan worden voorkomen dat onnodige verzameling en verdere verwerking (art. 13 Wbp) kunnen plaatsvinden[14].

'Opt-out'-mogelijkheid bij de registratie van NL-domeinnamen van particulieren
Bij de registratie van persoonsgebonden domeinnamen moet als gevolg van de inwerkingtreding van de Wbp de mogelijkheid worden geboden om zich tegen openbaarmaking van persoonsgegevens te verzetten, de zogenaamde 'opt-out'-mogelijkheid. Hierdoor zal naast een publiek WHOIS-deel een besloten deel van het SIDN-register worden gevoerd. De persoonsgegevens van iemand die gebruik heeft gemaakt van deze 'opt-out'-mogelijkheid, zijn in de WHOIS-database vervangen door de gegevens van diens internetprovider[15].

Zelfregulering

Voor de handhaving van de Wbp ziet het College een belangrijke rol weggelegd voor zelfregulering. Deze zelfregulering houdt in dat binnen organisaties en brancheverenigingen afspraken worden gemaakt over de invulling van de plichten en te treffen maatregelen als gevolg van de Wbp.

Richtlijnen, gedragscodes en handleidingen

Enkele partijen lopen voorop in de vertaling van de Wbp in richtlijnen voor privacy op het internet. Vanuit haar rol als toezichthouder publiceerde de Registratiekamer onderzoeksrapporten en informatiebladen met achtergrondinformatie en toelichtingen op de Wbp. Daarnaast is een aantal overheidsorganen en maatschappelijke instellingen actief met het opstellen van gedragscodes. Zo hebben het Ministerie van Justitie[15], het Electronic Commerce Platform[16], de Consumentenbond[17] en VNO-NCW[18] reeds gedragscodes en handleidingen gepubliceerd, waarbij aandacht is besteed aan het verzamelen van persoonsgegevens via het internet.

Privacyzegels

Voor aanbieders van websites is een meer in het oog springend middel beschikbaar om kenbaar te maken dat de aanbieder privacyrichtlijnen hanteert. Een zogeheten privacywebzegel is een afbeelding op veelal de hoofdpagina van de site met een referentie naar het privacystatement. Enkele nationale en internationale voorbeelden van privacyzegels zijn het WebTraderzegel van de Consumentenbond, het Privacy Seal Program van TRUSTe[19], het Webseal en het BBBOnline Privacy Program van het Better Business Bureau[20]. Het toezicht van uitgevers van privacywebzegels houdt onder meer in dat ze eisen stellen aan de inhoud van het privacystatement en als intermediair fungeren bij klachten over houders van webzegels. Te veel klachten kan leiden tot het intrekken van het privacywebzegel door de uitgever.

Privacy Enhancing Technologies

Als nadere invulling van de te treffen beveiligingsmaatregelen op basis van artikel 13 van de Wbp heeft de Registratiekamer uitgebreid gepubliceerd over de inzet van zogeheten Privacy Enhancing Technologies (PET)[21]. De doelstelling van PET is tweeledig. Enerzijds dient de inzet van PET bij te dragen aan het elimineren of verminderen van persoonsgegevens in informatiesystemen en anderzijds aan het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens, zonder dat in beide gevallen sprake is van verlies van de functionaliteit van het betreffende informatiesysteem. In een motie is de regering opgeroepen het voortouw te nemen bij de inzet van PET bij haar eigen verwerking van persoonsgegevens. Het belangrijkste initiatief voor de ontwikkeling van PET gericht op het internet is het PISA (Privacy Incorporated Software Agent)-project[22]. Dit project bestaat uit een internationaal consortium van onderzoeksinstellingen en bedrijven dat zich tot doel heeft gesteld voor 2002 een PET-toepassing te ontwikkelen voor het internet op basis van intelligente software agents. Deze software agents zijn programma's die bepaalde taken voor de eigenaar van de agent vervullen, zonder dat directe input of toezicht van de eigenaar nodig is. De PISA heeft als taak alleen onder strikte voorwaarden de identiteit van de eigenaar vrij te geven en in alle andere gevallen alleen gebruik te maken van pseudoniemen. Daarnaast dient de PISA zich te kunnen authentiseren als 'bonafide' en voldoende beveiligd te zijn om zich te kunnen beschermen tegen ongeautoriseerd gebruik en andersoortige aanvallen vanaf het internet.

Met een privacywebzegel kan de aanbieder kenbaar maken privacyrichtlijnen te hanteren.

Een in opzet eenvoudige en reeds gerealiseerde toepassing van PET voor het internet is Tresparc Dominion, een digitale kluis op het internet waarin onder meer persoonsgegevens door de eigenaar zelf kunnen worden opgeslagen en onderhouden, en die alleen op aangeven van de eigenaar aan derden ter beschikking worden gesteld[23].

Toezicht

De verantwoordelijkheid voor toezicht op de naleving van de Wbp ligt primair bij de persoonsgegevensverwerkende organisaties. Het College ziet voor zichzelf slechts een tweedelijnsrol weggelegd. In het kader van deze zelfregulering kunnen organisaties een functionaris voor de gegevensbescherming aanstellen (art. 62 Wbp), aan wie de taak als toezichthouder op de naleving van de Wbp is gedelegeerd (art. 64 Wbp). Deze functionaris dient kundig en onafhankelijk te zijn, dient bij het CBP te zijn aangemeld en is verplicht tot geheimhouding ten aanzien van klachten of verzoeken (art. 63 Wbp).

Ook zijn door de Registratiekamer in samenwerking met de IT-audit-marktpartijen privacyauditproducten gedefinieerd. Deze auditproducten omvatten een privacy quickscan, een Wbp selfassessment vragenlijst en een raamwerk voor privacyaudits[24]. Organisaties dienen dus

Ir. R. de Wolf RE
is specialist op het gebied van de beveiliging van complexe heterogene netwerkinfrastructuren, internettoepassingen en midrangeplatformen als Unix, en Windows NT/2000. Daarnaast is hij betrokken bij opdrachten inzake penetratietests, IT forensics, intrusion detection en infrastructuurinventarisaties.

ook zelf opdracht te geven tot het laten uitvoeren van privacyonderzoeken door onafhankelijke partijen. Daarnaast is het streven van het College voor overheidsinstellingen de normen voor privacybescherming op te nemen in de toetsingskaders bij jaarlijkse audits door de externe IT-auditor.

De externe IT-auditor bevindt zich dus in een uitstekende positie om ondersteuning te bieden bij het toezicht houden op de naleving van de Wbp. Deze ondersteunende rol kan op een aantal manieren worden ingevuld. Zo kan de externe IT-auditor fungeren als een externe functionaris gegevensbescherming, ondersteuning bieden aan de interne privacyfunctionaris of de rol van lid van een commissie van toezicht vervullen[25] en mogelijk een webseal verstrekken.

Een meer vertrouwde rol van de IT-auditor is echter die van beveiligingsspecialist. In de beoordeling van en advisering over organisatorische en technische aspecten van informatiebeveiliging levert de IT-auditor een actieve bijdrage aan de realisatie dan wel toetsing van de op basis van artikel 13 vereiste beveiliging van persoonsgegevens. Zo kunnen internetaudits en -penetratietests een goed beeld geven van de mate waarin wordt voldaan aan de eisen in artikel 13.

Ten slotte

De Wbp heeft gevolgen voor alle vormen van het vergaren en bewerken van persoonsgegevens, dus ook via het internet. Omdat het internet vrijwel geen waarborgen biedt voor beveiliging van gegevens in opslag of tijdens transport, moeten aanbieders van internetdiensten nu extra aandacht besteden aan de beveiliging van persoonsgegevens op het net. De IT-auditor kan een belangrijke bijdrage leveren aan het toezicht op en de advisering over de naleving van de Wbp.

Referenties

1) http://www.vno-ncw.nl/privacy/, Vertrouwen op internet: Aarzeling consument staat doorgroei elektronische handel in de weg, opinieblad Forum, d.d. 21 februari 2001.
2) http://rechten.kub.nl/lom2/privacy/doc/wbp.pdf, Wet Bescherming Persoonsgegevens, Uitgave van *privacy*dossier.
3) http://www.rechtplein.nl/Privacy-aspecten.html, Overzicht privacyaspecten van e-business, Van Leeuwen & Van der Eerden Advocaten.
4) http://www.registratiekamer.nl/, Rapport 'Goed werken in netwerken'.
5) http://www.nisa-intellegence.nl/wiebes_hoorz.htm, Presentatie dr. Wiebes op Echelon-hoorzitting in de Tweede Kamer, 19 januari 2001.
6) http://www.privacyinternational.org/survey/, Privacy & Human Rights 2000, an international survey of privacy laws and developments.
7) http://www.mindef.nl/nieuws/media/content/190101_notitie/html, Notitie 'Het grootschalig afluisteren van moderne telecommunicatievoorzieningen', 19 januari 2001.
8) http://www.netkwesties.nl/editie15/artikel12.html, Zoeksystemen verzamelen gebruikersgegevens, Magazine over vrijheid, rechten en regels op het internet, 26 mei 2001.
9) http://www.franken.de/users/tentacle/papers/search-privacy.txt, Search Engines and Privacy, Marc Roessler, 28 maart 2001.
10) http://webveil.com/matrix.html, Anonymous Proxy Guide, updated 4 December 2000.
11) http://www.w3.org/P3P/, 'Platform for Privacy Preferences (P3P) Project', World Wide Web Consortium.
12) http://www.wired.com/news/print/0,1294,43686,00.html, MS Gets Privacy-Happy With New IE, Wired News, May 15, 2001.
13) http://www.minjus.nl/a_beleid/fact/handleidingwbp.pdf, Handleiding voor verwerkers van persoonsgegevens, Sauerwein en Linnemann, januari 2001.
14) http://www.surfnet.nl/publicaties/privacybrochure/, Privacyaspecten van Directory Services, SURFnet.
15) http://www.domain-registry.nl/p10081999.html, NL-domeinnamen van en voor particulieren, Aalberts, Prins en Schreuders, KUB CRBI, augustus 1999.
16) http://www.ecp.nl/trust/gedrag.htm, Model Gedragscode voor elektronisch zakendoen Draft versie 3.0.
17) http://www.dedigitaleconsument.nl/, Privacygedragsregels voor internetbedrijven en de WebTrader-richtlijn, 24 januari 2001.
18) http://www.vno-ncw.nl/download.html?code=207, Brochure Bedrijf, consument en privacy, januari 2001.
19) http://www.truste.com/programs/pub_how.html, Privacy Seal Program, TRUSTe.
20) http://www.bbbonline.com/privacy/index.asp, About the Privacy Program, Better Business Bureau.
21) http://www.registratiekamer.nl/bis/top_1_4_8.html, Mag het een bitje meer zijn? Brochure over (het gebruik van) Privacy Enhancing Technologies, de Registratiekamer, april 2001.
22) http://www.tno.nl/instit/fel/pisa/, Privacy Incorporate Software Agent (PISA), Building a privacy guardian for the electronic age, TNO FEL.
23) http://www.tresparc.nl/, Tresparc Dominion, de digitale kluis op het internet.
24) http://www.registratiekamer.nl/download/PAGEHEEL.PDF, Wbp, Samenwerkingsverband Audit Aanpak / Werkgroep Privacy Audit.
25) http://www.isaca.nl/newsletter/002xxx.htm, Implementatie Wbp medio 2000, verslag ISACA round table door T.O. Mos CISA RE RI, 10 januari 2000.