



Veel bedrijven zijn bang voor toezichthouders

Het organiseren van overheidstoezicht op geautomatiseerde informatiesystemen is geen eenvoudige zaak. Er zijn niet simpel twee partijen: de overheid en het bedrijfsleven, zegt Remco van Wijk. ICT maakt wel een geheel nieuwe wijze van toezicht mogelijk. En die stelt meer voor dan het omzetten van een analogo dossier naar een digitaal dossier.

Geautomatiseerde bedrijfsgeïnformatiesystemen bevatten vaak een schat aan informatie voor toezichthouders. Het grootste gedeelte van de bedrijven is nalevingsgezind en heeft belang bij een ongestoorde productie of dienstverlening. Het ligt daarom voor de hand dat deze bedrijven toezichthouders toegang geven tot hun informatiesystemen. Een toezichthouder, via zijn desktop aangesloten op een bedrijfsgeïnformatiesysteem, zou vanachter zijn bureau een analyse kunnen maken van het te verwachten nalevingstekort bij een bedrijf. Wanneer de analyse uitwijst dat een goede naleving waarschijnlijk is, kan de toezichthouder het aantal fysieke bezoeken beperken. Wanneer de analyse onwenselijke gebeurtenissen doet vermoeden, steekt hij wat vaker op de bedrijfslocatie zijn licht op. Private controlesystemen vormen dan met behulp van ICT een wezenlijk onderdeel van het overheidstoezicht. Dit past volledig in de doelstellingen die de overheid zich heeft gesteld op het gebied van e-government en toezicht op controle. Het op grote schaal herinrichten van het toezicht volgens dit model blijkt echter niet altijd even makkelijk.

In de afgelopen jaren zijn verschillende overheidsstukken verschenen waarin wordt ingegaan op toezicht op controle. De overheid wil het bedrijfsleven meer ruimte geven zelf de controle op naleving te organiseren. De overheid verwacht van bedrijven dan wel inzage in hoe zij het beoogde niveau van naleving

denken te garanderen. Dit kan bijvoorbeeld middels certificering van erkende kwaliteitssystemen of zogenaamde gidsen van goede praktijken. De overheid trekt zich gedeeltelijk terug uit het toezicht op de naleving zelf en richt haar toezicht met name op het functioneren van de bedrijfsgeïnformatiesystemen. ICT kan in dit kader een belangrijke rol spelen in de communicatie tussen de overheid en het bedrijfsleven, met dit probleem dat 'de overheid' en 'het bedrijfsleven' niet bestaan. Op het gebied van ICT is de diversiteit van partijen die betrokken zijn bij het overheidstoezicht groot. Sommige bedrijven bezitten geavanceerde geautomatiseerde informatiesystemen die voortdurend metingen uitvoeren bij kritische controlepunten. Andere bedrijven hebben met moeite bij de administratie een computer naar binnen kunnen slepen. Aan overheidszijde geldt dezelfde variatie. Elk bedrijf heeft te maken met verschillende toezichthouders. Toezichthouders die begonnen zijn als traditionele keurmeesters zullen over het algemeen meer moeite hebben de fysieke controles te verminderen en over te gaan op systeemtoezicht, dan de toezichthouders die binnen hun vakgebied eerder met digitale systemen te maken kregen. Kortom, de rol die de ICT kan spelen in het toezicht op controle verschilt per bedrijf en per toezichthouder. De implementatie van een collectief systeem is op korte termijn niet aan de orde. Veel bedrijven zijn terughoudend in het toegang verlenen van toezichthouders tot hun systemen. Zij

wachten liever een duidelijk, afgebakend informatieverzoek af. Dit betekent over het algemeen niet dat deze bedrijven niet aan wet- en regelgeving willen voldoen. Zij vrezen echter een toezichthouder die de ganse dag in de bedrijfssystemen aan het spitten is teneinde maar iets onrechtmatig boven tafel te krijgen. Deze angst leidt ertoe dat bedrijven vaak de mening zijn toegedaan: 'hoe minder informatie een toezichthouder heeft, hoe beter.' Dit wantrouwen jegens de toezichthouder komt niet zomaar uit de lucht vallen. Bij toezichthouders leeft vaak het idee dat meer informatie altijd beter is. Dit lijkt des te meer te gelden wanneer het toezicht op afstand plaatsvindt. De hoeveelheid informatie zegt echter

gerichter kunnen worden uitgevoerd wanneer een toezichthouder gevoed wordt met informatie uit andere schakels van een productieketen. Een voorbeeld. Een monster van een partij diervoeder geeft, net als bloedproef van levend vee, informatie over welke stoffen zich wel of niet in de voedselketen bevinden. Op basis van (het ontbreken van) informatie uit deze schakels uit de vleesketen, kunnen de keuringsinstellingen op een slachthuis worden opgevoerd of juist worden beperkt. Niet de eigen fysieke waarneming, maar een veilige, betrouwbare, rechtmatige en geautomatiseerde uitwisseling van gegevens vormt de ruggengraat van dit nieuwe toezicht. Specialisten uit de traditionele toezichtspraktijk

toezicht. Het is hierbij noodzakelijk dat zij gebruikmaken van (markt)kennis over ICT-gebruik en ICT-beveiliging. De blauwdruk bevat de eisen waar bedrijfsgeïnformatiesystemen aan moeten voldoen om in aanmerking te komen voor het nieuwe toezicht. Verder wordt aangegeven welke gegevens op welke wijze en op welk moment beschikbaar moeten zijn voor de verschillende toezichthouders. Belangrijk is dat de blauwdruk ook ingaat op de wijze waarvoor gegevens gebruikt gaan worden en welke procedures gevolgd gaan worden bij onregelmatigheden. Toezichthouders hebben de plicht aan te geven hoe een veilige gegevensoverdracht tussen bedrijven en toezichthouders en tussen toezichthouders onderling geborgd wordt en hoe zij garanderen dat de gegevens alleen volgens afspraak binnen de overheid gebruikt worden. De blauwdruk moet bedrijven inzicht geven in hoe het nieuwe toezichtregime zich wat betreft opbouw van toezichtlasten verhoudt tot het vigerende toezicht. Op basis van de aangegeven lasten kunnen zij bepalen of zij willen investeren in hun bedrijfsgeïnformatiesystemen en of zij de toezichthouders de vereiste toegang tot deze systemen willen verlenen. Kortom, samenwerken, vertrouwen en ICT vormen de sporten van de ladder naar het nieuwe toezicht.

REMCO VAN WIJK
AG • 13-07-'07

Remco van Wijk MSc is werkzaam bij Duthler Associates als adviseur ICT en beleid. Hij was eerder als adviseur betrokken bij het project 'Eenduidig Toezicht' in het domein 'De Vleesketen'.

Van collectief controlesysteem is op korte termijn geen sprake

niets over de betrouwbaarheid ervan. Dit geldt voor toezicht op locatie en voor toezicht op afstand. Natuurlijk kun je ter plaatse nog wat cijfers verifiëren en wil je voor een risicoanalyse op afstand misschien wat extra kruisverbanden controleren, maar de verbalans van drie maanden geleden, blijft de verbalans van drie maanden geleden, of deze nu op locatie uit de printer komt of automatisch in het systeem van de toezichthouder wordt weggeschreven. Bedrijven staan dus niet te wachten op een toezichthouder met volledige toegang tot het bedrijfsgeïnformatiesysteem en toezichthouders nemen niet snel genoegen met een beperkte toegang. Het gevolg is een patstelling die alleen verliezers kent.

Spookbeelden

In het kader van toezicht wordt het gebruik van ICT vaak te beperkt opgevat als een mogelijk hulpmiddel om de reeds bestaande toezichtsactiviteiten en -processen te vereenvoudigen. Een digitaal dossier: dezelfde indeling, maar geen gerommel met pen en papier. Geavanceerde meetinstrumenten: dezelfde metingen, maar geen tijdsverlies door omslachtige dataverwerking. ICT maakt echter een geheel nieuwe wijze van toezicht mogelijk. Dit toezicht kenmerkt zich door een optimaal gebruik van gegevensbronnen van private partijen en toezichthouders. Het omzetten van een analogo dossier naar een digitaal dossier is voor dit nieuwe toezicht niet voldoende. Betrokken partijen moeten gezamenlijk toegang krijgen tot een digitaal dossier dat voor de verschillende gebruikers een verschillende weergave kent. Voor sommige metingen zal bij het nieuwe toezicht gelden dat zij veel

hebben vaak weinig kennis van de mogelijkheden en beperkingen van ICT om zich een realistisch beeld te vormen van dit nieuwe toezicht. Hierdoor is er ruimte voor ongefundeerde spookbeelden. Zo roept toezicht op afstand door gebruik van gegevens uit een bedrijfsgeïnformatiesysteem het angstbeeld op van een situatie waarbij een bedrijf virtueel in orde lijkt, maar in werkelijkheid er een potje van maakt. Ook bij het nieuwe toezicht blijven toezichthouders gedwongen af en toe een kijkje in het veld nemen, maar juist ten aanzien van deze veldbezoeken geldt dat door het gebruik van ICT toezichthouders veel efficiënter een beeld kunnen vormen van hoe de gegevens uit bedrijfsgeïnformatiesystemen zich verhouden tot de werkelijkheid.

Blauwdruk

Voor een brede implementatie van het nieuwe toezicht is het essentieel dat toezichthouders op het gebied via ICT beter gaan samenwerken. Gezamenlijk zullen zij zich de komende jaren moeten richten op de sectoren waar de bedrijfsgeïnformatiesystemen over het algemeen van dusdanige kwaliteit zijn, dat zij zich lenen voor het nieuwe toezicht. Aan de hand van een risicoanalyse moeten bedrijven en toezichthouders de aspecten van de wet- en regelgeving bepalen waar een grote overeenkomst bestaat tussen publiek en privaat belang. Grote bedrijven in de vleesketen willen bijvoorbeeld veel energie steken in het borgen van de voedselveiligheid; zij hebben immers geen belang bij een voedselchandaal. Voor de geselecteerde gebieden moeten de toezichthouders komen tot een integrale blauwdruk van het nieuwe



Optimaliseren door ICT

Er is een enorme optimalisatieslag te maken wanneer toezichthouders ICT inzetten om optimaal gebruik te maken van de informatie die wordt verzameld bij een bedrijfsbezoek. Toezichthouders kunnen gezamenlijk een informatiesysteem gebruiken waarin bedrijven worden ingedeeld in verschillende risicoklassen, bijvoorbeeld groen, oranje en rood. Wanneer bijvoorbeeld het aantal vervuilingseenheden gemeten door de waterschappen bij een bezoek in lijn is met het aantal vervuilingseenheden weergegeven in het bedrijfsgeïnformatiesysteem, behoudt het bedrijf voor alle toezichthoudende instanties de status groen. Anders wordt het wanneer de VROM-inspectie op bezoek komt en merkt dat de gegevens uit het logboek hoerend bij de koelinstallaties niet sporen met de automatisch doorgekregen gegevens. Het bedrijf kan geen bevredigende verklaring geven voor dit probleem en krijgt dientengevolge een code oranje in het door toezichthoudende instanties gedeelde informatiesysteem en kan de komende periode een hogere bezoekfrequentie van verschillende toezichthouders verwachten. Bij een bedrijf met status rood staat prompt de gehele inspectieclub op de stoep.

Voordat een dergelijk systeem geoperationaliseerd kan worden, zijn afspraken over de uitwisseling van gegevens tussen bedrijven en toezichthouders en toezichthoudende instanties onderling vanzelfsprekend uitermate belangrijk. Daarnaast moet er absolute duidelijkheid zijn over criteria die gelden voor de codes groen, oranje en rood. Misschien het allerbelangrijkste: wanneer gaat een bedrijf dat op oranje staat weer op groen? Transparantie in hoe er met onregelmatigheden omgegaan wordt, is essentieel voor het vertrouwen dat bedrijven en overheid in elkaar moeten hebben bij het geautomatiseerd delen van informatie.

CONFLICT

Waar partijen onderling zaken doen, liggen conflicten op de loer. Wat te doen als de een niet doet wat volgens de ander is afgesproken? Naar de rechter stappen is een mogelijkheid, maar in de praktijk leidt dit vaak tot slepende processen met hoge kosten en een onzekere uitkomst. Mediation kan uitkomst bieden. Elke vier weken schetst Ben Slijk van de Stichting Geschillenoplossing voor Organisatie en Automatisering (SGOA) in deze column een case uit de praktijk.

Auteursrecht

Conflicten over auteursrechtelijke kwesties zijn vaak eenvoudig te beslechten, maar lastig uit te leggen aan wie niet in de Auteurswet is ingewijd. Daarin staan bepalingen die voor ondernemers moeilijk te verteren zijn. Zo volgt op betaling niet vanzelfsprekend de eigendomsoverdracht en wordt gesproken over het kopen van software, maar blijkt er in juridische zin geen sprake te zijn van koop

en verkoop. Probeer maar eens uit te leggen aan een ondernemer dat de op zijn aanwijzingen gebouwde software, waarin zijn specifieke bedrijfsprocessen zijn verwerkt én waarvan hij de ontwikkelkosten volledig heeft betaald, niet zijn eigendom is. De vergelijking met de bouw van het bedrijfspand dringt zich op. Dat werd wel zijn eigendom. Maar de software die het hele proces plant, bestuurt en bewaakt

en die de financiële administratie verzorgt zou hem niet toebehoren? Het kon toch niet zo zijn dat de softwarebouwer de door hem betaalde software aan zijn concurrenten zou mogen doorverkopen. Met dat laatste ging de kortgedingrechter voor een flink deel met hem mee, maar de auteursrechten bleven bij de maker. De rechter baseerde zich in zijn uitspraak op de Auteurswet van 1912, die belangen van auteurs, kunstenaars en wetenschappers beschermt tegen uitbuiting. Er is bepaald dat auteursrecht ontstaat zonder dat er formaliteiten behoeven te worden vervuld. De enige eis is dat er sprake moet zijn van een nieuw en oorspronkelijk werk van letterkunde, wetenschap of kunst. Volgens artikel 10 van de Auteurswet valt daaronder ook computerprogrammatuur en het voorbereidend materiaal. Het overdragen van het auteursrecht is daarentegen gebonden aan de strikte regel dat de overdracht

schriftelijk (in een akte) moet zijn vastgelegd. En daar wringt de schoen. In de ICT-branche gaan contracten veelal over het ontwikkelen en leveren van software en komen de de auteursrechten zelden aan de orde. Als dat wel het geval is en partijen overeenkomen dat de rechten zullen toekomen aan de opdrachtgever, dan is het nog maar de vraag of die afspraak voldoet aan de eisen die de wet stelt. Zo kan de daadwerkelijke overdracht pas plaatsvinden nadat het werk is voltooid. Er moet dus, na de oplevering, nog een document worden opgemaakt en ondertekend waarin met zoveel woorden staat dat de auteursrechten op het werk worden overgedragen. Het stond de softwareleverancier in dit geval weliswaar niet vrij om de software in ongewijzigde vorm door te verkopen aan de concurrenten van de ondernemer. Dat zou volgens de rechter onrechtmatig kun-

nen zijn, maar de softwarebouwer heeft wel de mogelijkheid om het softwarepakket verder te vermarkten in aanpalende branches. Een beroep op de redelijkheid en de billijkheid door de teleurgestelde fabrikant faalde, want rechters mogen daarmee wel rekening houden, maar in dit geval laten de tussen partijen gesloten overeenkomst, de wet en de jurisprudentie daar geen ruimte voor. Bovendien waren de algemene voorwaarden van de Fenit van toepassing en die maken een expliciet voorbehoud ten aanzien van het auteursrecht. De opdrachtgever had zich de consequenties van het auteursrecht op software niet gerealiseerd. Overigens werkte de software naar tevredenheid, maar kon hij moeilijk verkopen dat waarvoor hij betaald had, zijn eigendom niet werd, maar een melkkoetje voor de leverancier.

BEN SLIJK
AG • 13-07-'07

