‘Het gemak waarmee gebruikers omgaan met vertrouwelijke informatie…’

Veiligheid, vertrouwelijkheid, betrouwbaarheid en (juridische) aansprakelijkheid zijn tegenwoordig de belangrijkste onderwerpen van gesprek in de boardrooms. Zekerheid over met wie je te maken hebt en welke informatie van wie afkomstig is, is cruciaal bij belangrijke beslissingstrajecten. Met terugwerkende kracht zou u zomaar aansprakelijk gesteld kunnen worden voor een beslissing, met verstrekkende gevolgen. Dan maar niets meer beslissen? ‘Dat is ook geen optie uiteraard. Het gemak waarmee desondanks wordt omgesprongen met belangrijke informatie baart mij echter wel zorgen’, aldus Gert Jan Knoet, onder meer docent aan diverse instellingen die zich bezighouden met verantwoord informatiebeheer in het algemeen en de elektronische handtekening in het bijzonder.

Gert Jan Knoet

Het digitale werken neemt hand over hand toe. Direct daaraan gekoppeld is de mate waarin informatie en de afzender betrouwbaar zijn. Zonder elektronische handtekening, met alle procedures en kanttekeningen erbij, is eigenlijk helemaal geen sprake van digitaal werken, vindt Knoet. ‘Een elektronische handtekening als puntje op de i, als kers op de taart bij digitaal werken wordt zwaar onderschat. Maar als je nu alle processen digitaal hebt en de informatie is digitaal, maar je moet een document nog steeds printen en handmatig ondertekenen of er staat een gescande handtekening onder het digitale document; hoe ver denk je dan eigenlijk dat je bent? In mijn ogen ben je dan nog net zo ver als vóór al die digitalisering. Een op de juiste manier elektronisch ondertekend document heeft een veel grotere juridische waarde. Dat wordt ook wel onderkend in de markt, maar niet wat daar voor nodig is.’

Discussie

Het is een beetje een rommeltje zo op het oog. Een digitale handtekening, een gescande handtekening, een elektronische handtekening, de termen vliegen je om de oren als je je erin gaat verdiepen. ‘Dat heeft alles te maken met de mate waarin je een bepaalde veiligheid en betrouwbaarheid wilt inbouwen in de ondertekening. Het is uiteraard een fluitje van een cent om een gescande handtekening onder

een document te plaatsen. Daarom heeft die geen enkele juridische waarde. Je kunt zo'n digitale handtekening wel gebruiken, maar dan intern of tussen werkmaatschappijen of zo. Er zijn echter genoeg organisaties die menen dat zo'n ondertekening gelijk staat met de 'natte handtekening'. Niet dus. Het grappige is echter, dat van zo'n natte handtekening, die tegenwoordig heel eenvoudig niet van echt te onderscheiden nagebootst kan worden met de huidige printtechnologie, de echtheid niet in twijfel wordt getrokken. Niet van de handtekening en niet van het document waar die onder staat. Dus staat daarmee ook de inhoud van zo'n document niet meer ter discussie. In het geval er een digitaal equivalent van die handtekening onder moet komen, moet de gebruiker ineens aan allerlei zware randvoorwaarden voldoen voordat deze wordt geaccepteerd. Die vorm van ondertekening is veel bureaucratischer. Daarom moet je voorafgaand aan de invoering van die elektronische handtekening goed nadenken over het verloop van je informatie- en beslisprocessen. Alleen dan kun je het digitaal ondertekenen van documenten en volledig digitaal werken op de juiste wijze toepassen.'

Wat is wat?

Er zijn drie soorten elektronische handtekening, ziet Knoet. 'De eerste is een gewone, niet gekwalificeerde handtekening. Dat zijn bijvoorbeeld een gescande handtekening of gewoon je naam onder een e-mail. Zelfs de zin 'dit bericht is elektronisch vervaardigd en daarom niet ondertekend', zoals de Belastingdienst vaak doet, valt in die categorie. Deze vorm heeft geen enkele juridische waarde, maar het geeft aan van wie het bericht of document afkomstig zou zijn. De tweede vorm is de geavanceerde elektronische handtekening. Die gaat een hele stap verder dan de eerste. De strekking ervan is echter nog steeds dat hoewel aantoonbaar is waar het document van komt, de juridische bewijslast nog steeds bij de verzender ligt. Er zijn overigens wel allerlei strikte voorwaarden aan deze manier van ondertekenen verbonden. De Wet elektronische handtekeningen stelt de volgende eisen: handtekening en ondertekenaar zijn op unieke wijze met elkaar verbonden; de handtekening maakt het mogelijk de ondertekenaar te identificeren; de manier van ondertekenen staat onder exclusieve controle van de ondertekenaar; en ten slotte, de handtekening is op dusdanige wijze met het bestand verbonden dat naderhand aangebrachte wijzigingen in dat bestand kunnen worden opgespoord.' Voor wie echter een waterdichte methode wil om een document digitaal te ondertekenen is overgeleverd aan de derde vorm, de gekwalificeerde (gecertificeerde) elektronische handtekening. Knoet: 'Alleen met deze methode heb je een juridisch waterdichte zaak als er een dispuut ontstaat. De bewijslast ligt dan bij de andere partij en niet bij jezelf.'

Waterdicht

Die derde methode behelst dat Trusted Third Parties (TTP's) als certificaatverstrekkers een unieke code koppelen aan een unieke gebruiker en leggen dat vast in een

digitaal certificaat. Het certificaat verbindt de gegevens voor het verifiëren van de handtekening aan een bepaalde persoon en bevestigt daarmee de identiteit van die persoon. Gekoppeld aan die laatste vorm van ondertekening is de zogenaamde PKI-infrastructuur. Knoet: 'PKI (Public Key Infrastructure) geeft garanties omtrent de communicatie met een onbekende partij. PKI geeft je de zekerheid dat je te maken hebt met de persoon die de ander beweert te zijn. Praktisch gezien is PKI een set van technische en organisatorische voorzieningen, waarmee versleuteling van berichten wordt ondersteund. Die berichten kunnen dan niet 'zomaar' worden gelezen. Daarvoor is 'de sleutel' nodig. Het komt erop neer dat de verzendende partij de ontvangende partij via zo'n TTP een sleutel geeft om zijn berichten te kunnen ontvangen en lezen. Zo'n derde partij, TTP, moet de identiteit bevestigen van de eigenaar van een bepaalde sleutel, zodat iedereen van elkaar weet wie het is. Deze TTP's staan vervolgens onder toezicht bij de Onafhankelijke Post en Telecom Autoriteit (OPTA).'

Altijd een zwakke schakel

Dat het desalniettemin toch nog weleens fout kan gaan, heeft de hele affaire met DigiNotar wel bewezen. Knoet: 'Als je wilt frauderen, kun je frauderen. Het gaat er in alle gevallen echter om dat als je voor de rechter staat je kunt aantonen dat je als goed huisvader hebt gehandeld. Dat je ervoor hebt gezorgd en alles in het werk hebt gesteld om de juiste informatie op de juiste manier bij de juiste mensen af te leveren. Er is echter altijd wel een zwakke schakel en in de meeste gevallen is dat de medewerker zelf, iemand die het systeem niet goed gebruikt. Dat is precies de reden van de kop boven het verhaal: ik maak mij daar zorgen over. Het gemak waarmee medewerkers denken dat 'het wel is geregeld' is op zijn minst verontrustend. Ik heb het al heel vaak in de praktijk meegemaakt dat men al snel denkt dat alles waterdicht is afgetimmerd. Terwijl dat in de verste verte niet het geval is. Als ik zie dat bij bepaalde organisaties de iPads je om de oren vliegen en mensen daar van alles mee kunnen (en mogen!) doen, zowel privé als werk, dan slaat de schrik mij om het hart. Hoe is de toegang tot die apparaten en de servers van de organisatie geregeld? Wie geeft aan wanneer een regel wordt overtreden? Welke bedrijfskritische informatie staat er op die iPad van de medewerker? Plaats- en tijdonafhankelijk digitaal werken is dan wel mooi en zeker niet meer terug te draaien, maar er komt wel wat meer bij kijken dan alleen een set iPads naar binnen rollen. Maar ook gewoon op de vaste werkplek: weglopen van je pc en dan het scherm aan laten staan, dus geen vergrendeling. Onderzoek heeft uitgewezen dat dat soort zaken (social engineering, even snel de pc van iemand anders

gebruiken, want ik heb de mijne net afgesloten) veel voorkomen. Dat kan enorme schade veroorzaken, afhankelijk van de soort informatie die op dat moment 'wordt gedeeld'.'

Vooronderzoek

Knoet is fanatiek pleiter voor een gedegen vooronderzoek naar alle ins en outs van de organisatie wanneer het gaat om het toepassen van de elektronische ondertekening van berichten of documenten, en daarmee dus het verder uitrollen van digitaal en plaats- en tijdonafhankelijk werken. 'Voordat je daarmee verder gaat, moet je een helder beeld hebben van de risico's en de doelstellingen. Zowel van de huidige manier van werken als van de beoogde. Gaat het om relatief risicoloze uitwisseling van documenten onderling, dan kun je overwegen om de eerste optie van een digitale handtekening te gaan gebruiken. Gaat het echter om cruciale informatie, waaraan belangrijke beslissingen met verstrekkende gevolgen worden gekoppeld dan is het zaak zo ver te gaan als je kunt om elke zekerheid die je kunt krijgen in te bouwen…'

Er zijn vier aspecten die volgens Knoet onder de loep moeten worden genomen tijdens zo'n vooronderzoek. 'Het gaat om de processen, de organisatie, het juridisch kader en de ICT. Maar het gaat vooral om veranderen. Dit soort trajecten draaien voor 80% om veranderen en voor 20% om ICT. Want uiteindelijk komt er wel/ook ICT bij kijken. Laat de aanstaande gebruikers zien wat de impact is van de nieuwe manier van werken; laat processen simuleren, zodat ze stap voor stap kunnen meekijken en ervaren wat het verschil is.'

Elektronische handtekening is slechts het begin

Als een organisatie daadwerkelijk de stap wil zetten naar volledig digitaal werken, dan ontkomt die niet aan een nauwkeurig onderzoek naar al het voorgaande, aldus Knoet. 'Het lijkt erop, dat het invoeren van een elektronische handtekening wordt gezien als het laatste losse eindje van digitaal werken. Het is juist het begin! Het is de start van een nauwgezette analyse van waar je staat als organisatie met betrekking tot digitaal werken, digitaal informatiebeheer en plaats- en tijdonafhankelijk werken. Dat doe je niet zomaar even op vrijdagmiddag bij de borrel. Het heeft vergaande consequenties en het kan ook alleen werken als de hele organisatie erachter staat. Als er een 'ontsnappingsroute' is om niet langs de afgesproken weg te werken, dan zullen criticasters die weg volgen. Iedereen moet dus overtuigd zijn van het belang van de juiste toepassing en het volgen en borgen van procedures voor het invoeren van digitaal ondertekenen en dus digitaal werken. Ook voor de langere termijn moeten er garanties zijn voor een (duurzaam) verantwoorde manier van omgaan met digitale informatie. In een tijd waar identiteitsfraude bijna aan de orde van de dag is, wordt het maken en volgen van goede afspraken van het grootste belang. Vertrouwelijkheid en informatiebeveiliging zijn hét issue voor de komende jaren.'

'En voor iedereen die denkt dat hij voor zichzelf alles op orde heeft: hoe vaak heeft u uw handtekening ergens op uw computer staan, of een kopie van uw identiteitsbewijs…..?'