E-mailverkeer en de kernwaarden van de Rechtspraak

Prins, Corien

Published in:
Nederlands Juristenblad

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

E-mailverkeer en de kernwaarden van de Rechtspraak

1 Sinds de Amerikaanse verkiezingen kan niemand nog beweren dat e-mailcorrespondentie via een publiek netwerk (veelal internet) veilig is. Luttele weken na de overwinning van Trump oordeelde de Hoge Raad welwillend over het gebruik van e-mail voor het toezenden van een machtiging aan de griffie van de rechtbank om hoger beroep in te stellen.[1] Het arrest ziet niet op de rechtmatigheid van het gebruik van het medium e-mail als zodanig, maar biedt wel een mooie kapstok voor de vraag of het überhaupt veilig is om per e-mail met en binnen de Rechtspraak te communiceren. En dat agendeert of processtukken langs deze weg zijn te versturen dan wel een concept-vonnis via de privémail aan een collega valt voor te leggen.

Veilig is privé e-mail allerminst. We weten inmiddels allemaal dat verzending van berichten via een publiek netwerk kwetsbaar is voor phishing en ander misbruik van (persoons)gegevens. De overheid is zich daar van bewust. Afgelopen zomer nog meldde minister Plasterk in antwoord op Kamervragen dat een extra impuls wordt gegeven aan het implementeren van beveiligingsstandaarden. Het streven is dat overheden de nieuwe standaarden per eind 2017 hebben geïmplementeerd. Aanleiding vormde een steekproef van het tijdschrift *Binnenlands Bestuur* waaruit bleek dat gemeenten de uitgevaardigde standaarden voor veilig e-mail nauwelijks gebruikten. Van de vijftig onderzochte gemeenten bleken alleen Den Haag, Woerden en Den Bosch die standaarden aan te houden.

Wat zou het beeld zijn als een dergelijk onderzoek bij de gerechten wordt uitgevoerd? Hoe vaak mailen rechters elkaar een concept-vonnis via een publiek netwerk in plaats van via de beveiligde omgeving? Wat is het beeld als we kijken naar het berichtenverkeer vanuit het OM naar het kabinet Rechter-Commissaris of naar de communicatie met de Raden voor de Kinderbescherming? Maken griffiers trouw gebruik van de beveiligde omgeving van de Rechtspraak als ze concepten van conclusies of scans van bijbehorende processtukken naar bijvoorbeeld een AG versturen? De realiteit van alledag is dat ook binnen de rechterlijke macht werk wordt verzet met behulp van de smartphone, ipad of eigen laptop. Dat kan, maar dan wel met gebruikmaking van de beveiligde omgeving. En die is beschikbaar. Voor de buitenwereld met de stapsgewijze implementatie van KEI. Voor rechters, griffiers en andere medewerkers van de rechterlijke macht met het al langer beschikbare REP beveiligingsprotocol, waarmee (ook vanuit huis) intern kan worden gecommuniceerd.

KEI introduceert een beveiligde omgeving voor onder meer het indienen van processtukken. Het gebruik van een publiek netwerk voor indiening is daarmee niet langer mogelijk. De Wet digitale processtukken (*Stb*. 2016, 90) sluit het gebruik van e-mail voor de rechtsgeldige indiening namelijk expliciet uit. E-mail kan uitsluitend worden benut om zgn. notificaties te verzenden: een bericht naar de ontvanger dat er een nieuw bericht of een nieuwe handeling op hem staat te wachten in het beveiligde portaal waarop actie wordt verlangd. De achterliggende reden om in dit geval wel te kiezen voor e-mail is dat van een incidentele gebruiker immers niet kan worden verwacht dat hij continue het digitale portaal van de Rechtspraak checkt.

Evenals gemeenten, heeft ook de Rechtspraak standaarden voor veilig e-mail uitgevaardigd. Rechters, griffiers en andere medewerkers moeten gebruik maken van het zgn. REP protocol als ze processtukken, concepten van conclusies en andere documenten intern versturen. En zoals vele andere organisaties heeft ook de Rechtspraak regels gesteld voor het gebruik van e-mail voorzieningen. Zo is het medewerkers verboden informatie te sturen naar een privé e-mailadres waarbij de verzending via het publieke internet plaatsvindt of over een niet-publiek netwerk dat niet voldoet aan de eisen van beveiliging die door de Rechtspraak zijn gesteld. Afgaande op signalen vanuit de rechterlijke macht is de kans echter reëel dat rechters – net als gemeente-ambtenaren – de uitgevaardigde standaarden voor veilig e-mail lang niet altijd gebruiken. Maar afgezien van het gehoor geven aan (en door de presidenten onder de aandacht brengen en handhaven van!) de interne gedragsregels: zouden de betrokkenen zich realiseren dat mailen buiten de beveiligde omgeving om een datalek conform art. 34a Wet bescherming persoonsgegevens oplevert? Belangrijk is namelijk dat het bij een datalek niet alleen gaat om het vrijkomen (lekken) van persoonsgegevens, maar ook om de onrechtmatige verwerking van persoonsgegevens. En daar is onder meer sprake van als de gegevens zijn blootgesteld aan een verwerking waartegen beveiligingsmaatregelen (zoals het REP protocol) bescherming moeten bieden.

Bij de Rechtspraak gaat het om kwetsbare dossiers met gevoelige gegevens. Gegevens die de positie van individuen en bedrijven raken en potentieel enorm kunnen raken. Dergelijke gegevens mogen niet op straat komen te liggen. Wie over deze dossiers en gegevens correspondeert via e-mailfaciliteiten die gebruik maken van een publiek netwerk neemt dan ook het risico dat de gegevens in verkeerde handen vallen. Maar wat mij betreft gaat het om veel meer dan uitsluitend het nemen van dit risico. Met dit handelen zijn namelijk ook de kernwaarden van de Rechtspraak in het geding. Wie deze kernwaarden beziet in het licht van zorgvuldige en integere digitale communicatie, weet dat het morele kompas van deze waarden de rechter en anderen binnen de rechterlijke macht wijst op de gevolgen en impact van hun handelen met moderne communicatiemiddelen. Kortom, een hedendaagse implementatie van de kernwaarden van de Rechtspraak impliceert dat alle bij de Rechtspraak betrokkenen gebruik maken van veilige communicatievoorzieningen. Rechters: een inhoudelijk mailtje versturen via Outlook of andere publieke systemen? Besef dat het in strijd is met uw kernwaarden.

Corien Prins

1. ECLI:NL:HR:2016:2654