Het ontwikkelen van e-mailconventies

Drs. W.J.P. van de Meent

De gevaren van e-mail manifesteren zich de laatste tijd meer dan ooit. Bijna maandelijks verschijnen in de pers wel mededelingen over virusverspreidingen die met een sneeuwbaleffect organisaties over de gehele aarde treffen. Afgelopen februari sloeg het 'Anna Kournikova'-virus over de wereld toe en vorig jaar mei teisterde het 'Iloveyou'-virus wereldwijd vele organisaties en veroorzaakte voor 7 miljard gulden schade.

Inleiding

Een groot aantal organisaties in Nederland heeft een e-mailfaciliteit voor zijn werknemers. Het wordt steeds duidelijker dat deze e-mailfaciliteit een aantal nadelen met zich meebrengt, zoals de zojuist genoemde virussen of het misbruik van e-mail voor persoonlijke zaken. De meeste nadelen zijn een gevolg van de aard van de communicatie via e-mail: deze is vaak informeel en berichtjes zijn zeer makkelijk te versturen. Ook is een aantal nadelen het gevolg van het feit dat het computernetwerk van de organisatie wordt verbonden met het internet.

Een organisatie kan de nadelen proberen te beperken door het implementeren van technische beveiligingsmaatregelen zoals firewalls of encryptie, maar alleen technische maatregelen zijn vaak niet afdoende. Door middel van een e-mailconventie kan men de werknemers expliciet wijzen op de nadelen die e-mail heeft. Overigens hoeft het doel van de e-mailconventie niet beperkt te zijn tot het wijzen op nadelen. Er kan ook aandacht worden besteed aan de mogelijkheden van e-mail en aan tips voor goed e-mailgebruik. De e-mailconventie wordt ook wel anders genoemd, zoals e-mailpolicy of e-mailgedragscode, maar in dit artikel zal over e-mailconventie worden gesproken.

De laatste tijd komt er in Nederland steeds meer aandacht voor e-mailconventies. Er heeft een aantal incidenten plaatsgevonden en steeds meer werkgevers raken geïnteresseerd in het onderwerp. Er worden jaarlijks congressen georganiseerd over deze materie en de Registratiekamer kwam in december 2000 met een publicatie met de titel *Goed werken in netwerken – Regels voor controle op e-mail en internetgebruik van werknemers* ([Regi01]). Veel organisaties blijken echter moeite te hebben om hun e-mailconventie zodanig vorm te geven dat deze ook echt werkt. De vraag is dus: hoe komt een organisatie aan een e-mailconventie en hoe zorgt men ervoor dat werknemers de conventie kennen en gemotiveerd zijn om zich te gedragen conform die conventie?

In dit artikel wordt ingegaan op de kenmerken, effecten en nadelen van e-mail voor organisaties. Er wordt in het kort een aantal technische beveiligingsmaatregelen geschetst die een organisatie kan implementeren om de gevolgen van de nadelen te beperken. Vervolgens wordt ingezoomd op e-mailconventies en wordt een door KPMG ontwikkelde fasering geïntroduceerd die door organisaties in Nederland gebruikt kan worden om een e-mailconventie te ontwikkelen. Deze fasering heeft een theoretische basis en is verder uitgewerkt aan de hand van een praktijkonderzoek.

Kenmerken van e-mail

Eén van de belangrijkste functies van e-mail is de mogelijkheid om een bericht te maken en te versturen aan één of meer gebruikers tegelijkertijd, dat vrijwel direct op de plaats van bestemming aankomt. Verder is het een asynchroon medium; de geadresseerde hoeft het bericht pas te lezen op het moment dat het hem uitkomt. Een asynchroon medium is zeer handig binnen organisaties, omdat er relatief veel korte, relatief onbelangrijke mededelingen worden gedaan of vragen worden gesteld. Door het sturen van een e-mail loopt de verzender niet het risico de geadresseerde te storen of hem afwezig te treffen.

Een tweede belangrijke functie is de mogelijkheid van het zogenaamde 'point-to-point'- en 'broadcast'-gebruik van e-mail. Vaak is e-mail 'point-to-point', wat inhoudt dat een gebruiker een bericht naar één andere gebruiker stuurt. Er is echter ook de mogelijkheid voor de verzender om vrij eenvoudig informatie te verspreiden door de hele organisatie tegen lagere kosten dan via andere media.

Een andere eigenschap van e-mail is dat de informatie in elektronische vorm bestaat. Dit houdt in dat de informatie kan worden gecreëerd, veranderd, verstuurd, ontvangen en gearchiveerd op een computer, wat veel praktische voordelen heeft.

E-mail wordt vaak gezien als een relatief informeel communicatiemedium. In principe kan een e-mailbericht net zo formeel zijn als bijvoorbeeld een op papier geschreven memo, maar de historie van e-mail heeft ervoor gezorgd dat dit medium informeler wordt gebruikt. Het eerste gebruik van e-mail gebeurde door wetenschappers, die de gewoonte ontwikkelden om informele en collegiale berichten te versturen. Dit informele karakter van e-mail is door de latere gebruikers, dus ook in organisaties, overgenomen. De tolerantie ten opzichte van spel- en grammaticafouten is bij e-mail groter dan bij geschreven bedrijfscommunicatie.

Effecten van e-mail

Van den Hooff ([Hoof98]) komt in zijn promotieonderzoek in navolging van Sproull en Kiesler ([Spro91]) taakgerelateerde ('eerste orde') en communicatiegerelateerde ('tweede orde') effecten van e-mail tegen.

Eerste orde-effecten:

* Werknemers blijken efficiënter te kunnen werken dankzij e-mail. In het onderzoek van Van den Hooff gaf een grote meerderheid aan meer te kunnen doen in minder tijd, sneller te kunnen werken en taken efficiënter te kunnen uitvoeren.
* Werknemers blijken efficiënter te kunnen communiceren dankzij e-mail. Een grote meerderheid bleek informatie efficiënter (makkelijker) op de juiste plaats te kunnen krijgen, zelf informatie efficiënter tot haar beschikking te krijgen en belangrijke contacten gemakkelijker te kunnen bereiken dankzij e-mail.
* Werknemers blijken beter (effectiever) te kunnen werken. De helft van de werknemers vond ook de kwaliteit van de eigen werkzaamheden en de informatie die men daarvoor nodig heeft, toegenomen.

Deze effecten worden vaak door het management gekwantificeerd en gebruikt om de investering in het e-mailsysteem te rechtvaardigen. Er wordt gekeken naar de directe baten. Dit is echter wel een kortzichtige manier om de investering te rechtvaardigen. E-mail heeft zich steeds meer ontwikkeld tot een groepsgeoriënteerd medium voor complexe communicatie. Daardoor wordt e-mail van strategisch belang voor organisaties en wordt e-mail essentieel voor de communicatieprocessen in een organisatie.

Tweede orde-effecten:

* Meer communicatie buiten de eigen organisatie. Een aantal werknemers geeft aan meer buiten de organisatie of de eigen organisatieafdeling te communiceren dan vroeger het geval was.
* Het opdoen van nieuwe contacten via e-mail. Door de laagdrempeligheid van e-mail en een grote voorraad mogelijke contacten op bijvoorbeeld het internet, doet een deel van de werknemers ook nieuwe contacten via e-mail op.
* Het ontstaan van een meer flexibele communicatiestructuur. E-mail blijkt minder formele communicatie in de hand te werken en direct contact te vergemakkelijken tussen personen die in de 'formele' communicatiestructuur wellicht alleen indirect contact met elkaar zouden hebben.

Niet alleen de omvang, maar ook de effecten van e-mailgebruik nemen toe.

Niet alleen het gebruik van e-mail blijkt in de loop van de tijd toe te nemen, maar ook de effecten van dit gebruik. Tevens wordt e-mail voor steeds meer activiteiten gebruikt, omdat de werknemers merken dat e-mail voor meer activiteiten geschikt is dan men aanvankelijk dacht. Zo ontstaan weer meer tweede orde-effecten.

Lucas ([Luca98]) noemt enkele mogelijke gevolgen van de meer flexibele communicatiestructuur die ontstaat als gevolg van e-mail. Zo zal deze nieuwe structuur ervoor kunnen zorgen dat de individuele bijdrage van een werknemer aan de informatiestromen binnen de organisatie steeds minder zal verschillen van de bijdrage van een in de hiërarchie hoger geplaatste werknemer. Het zal steeds minder vaak voorkomen dat een paar individuen de informatiestromen binnen een organisatie beheersen. Werknemers durven makkelijker te communiceren met het management via e-mail en zullen ook makkelijker negatieve informatie durven te communiceren naar het management of andere collega's. Men kan zich afvragen of dit nu als positief of negatief effect gezien moet worden. Dat zal verschillen per organisatie. Is bijvoorbeeld een duidelijke hiërarchie essentieel voor haar functioneren, dan kan dit 'democratiserings'effect van e-mail in de organisatie schadelijke gevolgen hebben.

Nadelen van e-mail

Gekeken naar de positieve ontwikkelingen die e-mail met zich meebrengt voor organisaties kan het voor veel organisaties een onmisbaar gereedschap worden. E-mail kent echter ook nadelen, waarvan onderstaand een groot aantal wordt behandeld.

Hacking
Iemand van buiten de organisatie kan inbreken in de mailserver van een organisatie en op deze manier bijvoorbeeld usernames en passwords achterhalen of mailtjes versturen uit naam van iemand anders ('spoofing', zie verderop). Ook kan iemand vanuit de organisatie inbreken in de mailserver van de eigen organisatie of die van een andere organisatie.

Virussen, Trojaanse paarden
Sommige virussen en Trojaanse paarden zijn relatief onschadelijk, andere kunnen een heel netwerk platleggen of harde schijven wissen. Zoals al eerder gezegd, zijn er de laatste paar jaar enkele gevallen bekend van via e-mail verspreide virussen die door hun eigenschap om zichzelf razendsnel te vermenigvuldigen ervoor zorgden dat systemen bij organisaties verstopt raakten. E-mails kunnen virussen en Trojaanse paarden bevatten en vormen dus op deze manier een risico. Ook hier geldt dat e-mails met virussen of Trojaanse paarden van buiten af kunnen komen, maar ook van binnen de organisatie naar buiten kunnen worden gestuurd.

Niet-toegestane software
Via e-mail kunnen niet-toegestane (of niet-geautoriseerde) software, plaatjes of andere bestanden de organisatie worden binnengehaald, eventueel beschermd door copyright. Ook hier geldt dat deze software van binnen de organisatie naar buiten kan worden gestuurd.

Aanstootgevend materiaal
Buiten het feit dat materiaal dat met e-mail wordt meegestuurd beschermd kan zijn door copyright, kan dit materiaal of de tekst in de e-mail zelf ook aanstootgevend zijn. E-mails kunnen pornografie, uitingen van racisme, seksistische opmerkingen, extreme politieke of religieuze meningen, etc. bevatten. Nog afgezien van het

feit dat dit voor collega's die onwetend deze e-mails ontvangen onprettig kan zijn, kan het ook schadelijk zijn voor het imago van een organisatie als dit soort e-mails openbaar bekend wordt. Ook is het mogelijk dat gedupeerden een schadevergoeding eisen van de organisatie.

Flaming
Flaming is het openbaar beledigen van iemand via e-mail. Het openbare karakter hiervan wordt bereikt door de e-mail in een publiekelijk toegankelijke nieuwsgroep te zetten of door vele personen een kopie van de e-mail te sturen.

Grote e-mails of grote hoeveelheden e-mails
Er kunnen (opzettelijk of niet) heel grote e-mails of grote hoeveelheden e-mails binnen een organisatie worden verstuurd of van buiten een organisatie binnenkomen. Dit kan onder andere het gevolg zijn van een virus, van een werknemer die een e-mail verstuurt naar al zijn collega's, van een hard- of softwarefout of van een denial-of-service-aanval (waarbij er door meestal meerdere personen van buiten de organisatie enorme hoeveelheden berichten naar een server worden gestuurd met de bedoeling deze plat te leggen). Het gevolg van dergelijke e-mails kan zijn dat mailservers en dergelijke verstopt raken en dat men veel tijd kwijt is met het verwijderen van niet gewenste berichten.

Junk mail
Als e-mailgebruiker kan men overspoeld worden met zogenaamde junk mail of 'spam'. Dit zijn mailtjes met aanbiedingen van bijvoorbeeld pornografisch materiaal of tips om snel geld te verdienen. Soms zitten er echter ook serieuze adverteerders tussen, die via e-mail op een goedkope en makkelijke manier veel mensen willen bereiken. Onder junk mail vallen ook de zogenaamde kettingmails (de elektronische variant van de kettingbrief). Al deze e-mails, ook die van de min of meer serieuze adverteerders, hebben een aanzienlijke irritatie tot gevolg bij de ontvangers en netwerkbeheerders. Een groot aantal van deze e-mails kan tot een aanzienlijke verstopping van het systeem leiden en tot een aanzienlijk tijdsbeslag voor het verwijderen ervan.
Vanzelfsprekend kunnen ook deze berichten van buiten de organisatie komen, maar ook vanuit de organisatie zelf verstuurd zijn.

Uitlekken van gevoelige informatie
E-mail via het internet kan worden gebruikt om vertrouwelijke data uit de organisatie te smokkelen, bijvoorbeeld naar een derde partij of naar een eigen e-mailadres thuis. Dit kan grote financiële schade of schade aan het imago van de organisatie opleveren.
Het verzenden van vertrouwelijke data hoeft overigens niet altijd opzettelijk te gebeuren. Het komt ook voor dat een werknemer in een adressenlijst per ongeluk een verkeerd adres selecteert en dit daarna niet meer controleert, waardoor gevoelige informatie bij de verkeerde persoon terechtkomt.

Spoofing
Spoofing is het verschijnsel waarbij iemand zich voordoet als iemand anders, dus bijvoorbeeld een e-mail vanuit het account van iemand anders stuurt. Dit kan mogelijk zijn geworden doordat iemand bijvoorbeeld zijn wachtwoord niet goed geheim heeft gehouden. Ook kan een hacker hebben ingebroken op iemands account binnen de organisatie. Iemand kan zo een andere persoon of organisatie veel schade berokkenen.

Misbruik van e-mail voor persoonlijke zaken
Er worden in een organisatie, net als bij de telefoon, veelvuldig persoonlijke berichten verstuurd via e-mail. Onder persoonlijke berichten worden berichten verstaan die in geen enkele relatie staan tot de uit te voeren werkzaamheden binnen het bedrijf.
Dit wordt pas echt een probleem voor de organisatie als het lezen en versturen van deze persoonlijke berichten duidelijk ten koste gaan van de productiviteit. De grote vraag hierbij is óf de organisatie persoonlijk gebruik van de e-mailfaciliteit binnen de organisatie toe moet laten en zo ja, wát de organisatie toe moet laten.
Tevens valt onder deze vorm van misbruik de werknemer die via e-mail contacten onderhoudt met de concurrent bij wie hij in dienst wil treden of die vertrouwelijke gegevens tegen betaling laat uitlekken.

Sterke afhankelijkheid van hard- en software
Eenmaal ingevoerd, kan e-mail een steeds belangrijker rol krijgen binnen de organisatie en onmisbaar worden voor de communicatie, zoals al eerder gezegd. Als er iets misgaat met het systeem kan dit betekenen dat de bedrijfsvoering stil komt te liggen, omdat de e-mailfaciliteit niet meer kan worden gebruikt.
Ook is er de mogelijkheid dat de overheid het computersysteem van een organisatie in beslag neemt tijdens het onderzoek van een rechtszaak waar de organisatie bij betrokken is (welke veroorzaakt kan zijn door misbruik van e-mail). Ook dan kan de bedrijfsvoering een flinke terugslag krijgen, omdat e-mailen niet meer mogelijk is.

Toenemende spanning tussen formele organisatiestructuur en dagelijkse praktijk
Zoals eerder gesteld in de paragraaf 'Effecten van e-mail', kan e-mail tot een verandering van de communicatiestructuur in een organisatie leiden. Dit kan een positief effect teweegbrengen, maar ook een negatief effect. Er kan een spanning ontstaan tussen enerzijds de formele organisatiestructuur en hiërarchie zoals die is vastgelegd en anderzijds de dagelijkse praktijk, die directer, informeler en minder controleerbaar gaat verlopen. Zo kan er bijvoorbeeld gemakkelijker communicatie plaatsvinden met relaties buiten de organisatie, zonder dat er een kwaliteitscontrole op deze communicatie plaatsvindt.

Door de laagdrempeligheid van e-mail kunnen medewerkers overspoeld raken met informatie.

Medewerkers krijgen te veel informatie te verwerken
Door de laagdrempeligheid van e-mail bestaat de kans dat medewerkers meer informatie te verwerken krijgen dan ze aankunnen. Juist omdat het zo makkelijk is om een e-mail te versturen, zullen veel mensen bij het versturen van een e-mail deze ook sturen aan mensen die 'misschien ook nog wel wat aan de informatie zullen

hebben'. Ook gebeurt dit wel omdat mensen zich willen indekken, in de trant van: 'Hij wist er ook van.'
Zo zijn medewerkers niet alleen kostbare tijd kwijt met het verwijderen van e-mails die weinig nuttige informatie bevatten, maar ook met het doorlezen en verwerken van e-mails die wel nuttige informatie bevatten, maar waarvan het te betwisten valt of zij nu juist ook deze informatie hadden moeten ontvangen.

Verdringing van persoonlijke contacten
Eerder werden de tweede orde-effecten van Sproull en Kiesler genoemd, namelijk de verandering van de communicatiepatronen binnen de organisatie. Een negatief aspect van deze veranderende communicatiecultuur is dat e-mail persoonlijke contacten in belangrijke mate gaat verdringen. Mensen zullen minder snel op hun collega afstappen, omdat het zoveel makkelijker is om even een e-mail te sturen. Hinde ([Hind99]) geeft aan dat dit niet altijd te maken heeft met luiheid of gemakzucht, maar dat werknemers zich gaan verstoppen voor collega's om conflict en andere vormen van contact te vermijden. Dit kan negatieve gevolgen hebben voor de werksfeer, bijvoorbeeld omdat conflicten niet duidelijk worden uitgesproken.

Juridische aansprakelijkheid
Per ongeluk of met opzet kunnen er virussen, aanstootgevend materiaal, vertrouwelijke informatie en dergelijke worden verzonden naar de verkeerde persoon of er wordt een bericht verzonden dat niet klopt, onvolledig is of nooit verzonden had mogen worden. Het komt voor dat geruchten binnen een organisatie via e-mail worden verspreid die een andere organisatie of een bepaalde persoon in diskrediet kunnen brengen. Dit gebeurt via e-mail veel vaker dan via bijvoorbeeld de telefoon, omdat e-mail blijkbaar de neiging opwekt bij mensen om veel eerder dat soort dingen te vermelden dan via de telefoon of in een persoonlijk gesprek ([Hind99]). Het gevaar is dat standpunten of meningen die door werknemers in een e-mail worden vertolkt, worden gezien als het standpunt of mening van de organisatie. Ook kunnen werknemers onbewust juridische verplichtingen aangaan.

Deze gebeurtenissen kunnen er allemaal toe leiden dat een organisatie juridisch aansprakelijk wordt gehouden voor wat haar werknemers doen. Dit is een groot risico. De naam van de organisatie van een verzender van een e-mail staat altijd ergens in de e-mail genoemd, dus de e-mails kunnen worden herleid naar de organisatie van herkomst. E-mails kunnen tevens worden toegelaten als bewijs in rechtszaken. Als dit gebeurt, betekent dit weer een potentiële schade aan het imago van een organisatie.

Grotere risico's bij externe e-mail

De meeste organisaties met e-mail hebben de mogelijkheid aan hun werknemers gegeven om extern via internet te kunnen mailen, omdat op deze manier ook met klanten en leveranciers kan worden gecommuniceerd en omdat er nieuwe contacten buiten de organisatie kunnen worden opgedaan. Het nadeel hiervan is dat het netwerk van de organisatie verbonden is met het onveilige internet, wat tot gevolg heeft dat de risico's een stuk groter worden. E-mails van buiten de organisatie kunnen binnenkomen en vice versa.

Beveiliging door middel van hard- en software

Een organisatie kan door middel van een aantal 'technische' beveiligingsmaatregelen, dat wil zeggen met hard- en software, proberen de gevolgen van de nadelen van e-mail te verkleinen.

Firewall
Een firewall kan worden gezien als een verdedigingslinie tussen het netwerk van de eigen organisatie en de buitenwereld. Het is een beveiligingsmaatregel op netwerkniveau. Al het verkeer tussen het netwerk van de organisatie en de buitenwereld (bijvoorbeeld het internet of een netwerk van een andere organisatie) wordt gedwongen langs deze firewall te gaan. Met een op de firewall geïnstalleerde mailfilter kan worden bepaald welke e-mails het netwerk binnen mogen komen en welke e-mails het netwerk mogen verlaten. Zo kunnen bijvoorbeeld e-mailberichten met een bepaalde grootte worden tegengehouden.
Ook kan een firewall zo worden geconfigureerd dat het interne netwerk onzichtbaar wordt voor gebruikers buiten de organisatie. Daardoor wordt het een stuk moeilijker om op het netwerk in te breken.

Beveiligingssoftware
Er is software beschikbaar die inkomende en uitgaande e-mails en de bestanden die worden meegezonden scant op bepaalde eigenschappen. Deze software, bijvoorbeeld een virusscanner, kan worden geïnstalleerd op een firewall, zodat de e-mails worden gecontroleerd die deze firewall passeren, maar ook de e-mails die zich op hardware in het netwerk bevinden. Buiten virusscanning is er software die scant op de inhoud van een bericht ('content scanning') en een melding geeft als een bepaald woord, een bepaald bestand of een bepaalde zin in een e-mail voorkomt.

Encryptie
E-mails kunnen voor verzending door middel van encryptie onleesbaar worden versleuteld of er kan een digitale handtekening worden toegevoegd. Zo kan bij ontvangst met meer zekerheid worden vastgesteld wie de e-mail verstuurd heeft en of deze ongewijzigd is gebleven gedurende transport; ook kan noch de verzender noch de ontvanger ontkennen dat de e-mail is verstuurd.

Disclaimers
Bij sommige organisaties wordt automatisch een zogenaamde 'disclaimer' onder e-mails geplakt die het eigen netwerk verlaten. Hieronder volgt een voorbeeld van zo'n disclaimer:
'Communicatie via internet is niet veilig en daarom accepteert de organisatie geen juridische aansprakelijkheid voor de inhoud van dit bericht. Alle zienswijzen of meningen in dit bericht zijn enkel die van de auteur en hoeven niet noodzakelijkerwijs die van de organisatie te verwoorden.'

Bij een aantal van bovenstaande beveiligingsmaatregelen zijn enkele kanttekeningen te plaatsen. Wat mag er in een disclaimer staan? Mag een organisatie de inhoud van de e-mail controleren? Is het gebruik van encryptie niet aan bepaalde voorwaarden verbonden? Aan dit soort vragen moet een organisatie zeker aandacht besteden.

Voorkomen is beter dan genezen. Een groot gedeelte van het probleem ligt bij het gedrag van de werknemers. De organisatie kan er beter voor zorgen dat werknemers zich netjes gedragen, dan dat ze door middel van allerlei technieken ongelukken moet zien te voorkomen. Dit kan de organisatie doen door het opstellen van een e-mailconventie, waarbij de organisatie er ook goed aan doet de hiervoor genoemde technische maatregelen erin te vermelden, als ze deze toepast. Hier moet men opmerken dat technische beveiligingsmaatregelen een aanvulling moeten zijn op de e-mailconventie, geen vervanging ([Brow99]).

E-mailconventie

Een e-mailconventie kan worden omschreven als een verzameling van tips, regels en/of andere zaken betreffende e-mail, bedoeld voor e-mailgebruikers in een organisatie. Het doel van een e-mailconventie is om uit te leggen wat de organisatie acceptabel gebruik vindt van e-mail en om werknemers en organisatie te beschermen tegen gevolgen van illegale acties en juridische aanklachten ([Gask98], [Nelm99]).

Hieronder volgt een voorbeeld-inhoudsopgave van een e-mailconventie om een overzicht te geven van welke onderwerpen kunnen worden behandeld in een dergelijke conventie.

1 Bedoeling van e-mail:
Voor welke doeleinden dient e-mail binnen de organisatie gebruikt te worden?

2 Goed omgaan met e-mail:
Tips voor het omgaan met e-mail en de applicatie.

3 Netiquette (algemene 'goed gedrag'-regels op internet):
Welke gedragsregels gelden er als je e-mails verstuurt, over het internet maar ook intern?

4 Privé-gebruik:
Wat voor regels gelden er als je privé-mail verstuurt?

5 Beveiliging door hard- en software: technische beveiligingsmaatregelen:
Welke technische beveiligingsmaatregelen zijn er genomen door de organisatie?

6 Misbruik en sancties:
Wat kan worden beschouwd als misbruik van de e-mailfaciliteit en wat zullen de sancties zijn bij misbruik?

Het proces van opstellen, inhoud bepalen en implementeren van een e-mailconventie verschilt per organisatie. Veel organisaties hebben hier moeite mee, wat onder andere blijkt uit het feit dat werknemers zich niet altijd aan de ingevoerde conventie blijken te houden en/of deze niet blijken te kennen. Hoe ontwikkelt men nu een e-mailconventie binnen een organisatie, zodanig dat de werknemers deze conventie als zinvol ervaren en zodanig dat de conventie handhaafbaar is en blijft?

Opzet praktijkonderzoek

Om een in de praktijk bruikbare ontwikkelfasering te kunnen ontwerpen, is er een praktijkonderzoek uitgevoerd. Er zijn bij zes Nederlandse organisaties elk drie personen geïnterviewd. Bij alle organisaties konden de werknemers gebruikmaken van e-mail. Zie tabel 1 voor een overzicht van deze organisaties.

Geïnterviewde organisaties	E-mailconventie aanwezig?
Overheidsdienst	Ja
Dienstverlenend bedrijf op het gebied van water, milieu en kwaliteitmanagement	Nee
Chemisch concern	Ja
Financiële dienstverlener	Ja
Luchtvaartmaatschappij	Ja
Automatiseringsbedrijf	Nee

Tabel 1. Geïnterviewde organisaties.

> Technische beveiligingsmaatregelen moeten een aanvulling zijn op de e-mailconventie, geen vervanging.

Bij elke organisatie zijn de volgende drie personen geïnterviewd:
* een verantwoordelijke manager of beleidsmaker, iemand die beleidsmatig verantwoordelijk is voor de e-mailconventie binnen de organisatie;
* een conventieopsteller, iemand die in opdracht van de beleidsmaker de conventie helpt opstellen, of daarbij wordt geraadpleegd;
* een willekeurige gebruiker, iemand die op geen enkele manier betrokken is geweest of zal worden bij het opstellen van de conventie en ook niet in de hogere lagen van de organisationele hiërarchie zit.

Aanvullend is er nog een interview bij de werknemersorganisatie FNV en bij de werkgeversorganisatie VNO-NCW afgenomen om daar de mening te peilen over dit onderwerp.

Tevens is er van enkele niet-geïnterviewde organisaties informatie verkregen, namelijk van:
* een accountants- en advieskantoor;
* twee IT-/automatiseringsbedrijven (allebei oorspronkelijk Amerikaans);
* een bank;
* twee ministeries.

Belangrijkste resultaten van het onderzoek

De resultaten van het onderzoek zijn globaal te verdelen in twee gebieden. Het ene beslaat de resultaten op het vlak van de kenmerken, effecten en nadelen van e-mail in organisaties. Het andere gebied beslaat de resultaten ten aanzien van e-mailconventies.

Kenmerken, effecten en nadelen

Alle kenmerken en effecten van e-mail eerder genoemd in dit artikel worden bevestigd bij de onderzochte organisaties. Wat betreft de nadelen werden de volgende als meest belangrijk onderscheiden:
* het te veel informatie moeten verwerken door medewerkers;
* het ontvangen en versturen van virussen en Trojaanse paarden;
* het ontvangen en versturen van een qua omvang grote e-mail of grote hoeveelheden e-mails.

Bovenstaande punten zijn gebaseerd op de resultaten van de interviews. Hierbij moet in overweging worden genomen dat een organisatie in interviews niet altijd alle incidenten aan wil/zal geven, omdat ze deze liever niet openbaar maakt.

Het gebruik van e-mail voor persoonlijke zaken en junk mail waren wel herkenbaar, maar werden niet zozeer als nadeel ervaren. Hacking en spoofing waren bij de geïnterviewde organisaties nauwelijks herkenbaar en werden ook niet als nadeel ervaren. De overige nadelen werden wel als bedreiging ervaren, maar in beperkte mate.

E-mailconventies

De meest opvallende zaken die bij het onderzoek naar voren kwamen waren de volgende:

* Een e-mailconventie wordt vrijwel altijd opgesteld ná het invoeren van e-mail. Een uitzondering hierop was de overheidsdienst. Het identificeren van de risico's en het anticiperen hierop is dus iets waar meestal niet direct aandacht aan wordt besteed.

* Bijna alle geïnterviewde personen vonden een e-mailconventie noodzakelijk, afgezien van enkele gebruikers en het FNV. Dit is belangrijk, want men kan zich afvragen of een conventie wel altijd noodzakelijk is in een organisatie.

* Beleidsmatig moet een conventie geplaatst worden binnen het informatiebeveiligingsbeleid en moet zij dus voornamelijk vanuit de 'risico'-kant benaderd worden, niet vanuit de 'mogelijkheden'-kant.

* Het opstellen van de e-mailconventie gebeurt niet alleen door de verantwoordelijke(n) voor informatiebeveiliging. Dit gebeurt in overleg met andere partijen binnen de organisatie, zoals een Personeelsafdeling, een Audit/Accountancy-afdeling en de ondernemingsraad. Ook kan er gebruik worden gemaakt van een PR-afdeling, omdat voor sommige communicatie via e-mail (bijvoorbeeld met klanten) bepaalde regels kunnen worden opgesteld.

* De e-mailconventie wordt soms geïntegreerd met andere regelgeving, zoals een conventie voor internetgebruik (feitelijk world wide web-gebruik), goed gebruik van IT of 'goed omgaan met informatie'.

* Alle organisaties hebben een virusscanner geïmplementeerd. Bij één organisatie wordt structureel gescand op inhoud. Encryptie wordt nog nauwelijks toegepast. Een disclaimer is aanwezig bij enkele organisaties evenals een automatische beperking op de grootte van de e-mails. Vooral het scannen op inhoud is een onderwerp waar veel discussie over is, vanwege het privacygevoelige karakter hiervan.

* De verhouding is ongeveer fiftyfifty wat betreft het accent van de conventie. De helft van de organisaties heeft een strikt verbiedende conventie. Bij de andere helft is de conventie meer stimulerend.

* De lengte van de conventie verschilt sterk per organisatie. Eén organisatie heeft een conventie van vijf regels, een andere organisatie heeft daar vijf pagina's voor nodig.

* In alle conventies wordt privé-gebruik van e-mail verboden. Er is echter geen enkele organisatie die handelt naar dit strikte verbod, privé-gebruik (met mate) wordt wel toegelaten. In het algemeen wordt er in de conventies wel vermeld wat als misbruik gezien wordt en wat hierop de sancties zijn. Overige zaken die voorkomen in de conventies zijn een vermelding van welke technische beveiligingsmaatregelen er zijn genomen en dat er verschillende klassen van informatie zijn wat betreft vertrouwelijkheid en hoe er met deze verschillende klassen moet worden omgegaan.

* Bij de gebruiker van één organisatie was de (wel aanwezige) conventie niet bekend. De gebruikers bij de andere organisaties kenden hun conventie wel, maar wisten niet altijd precies wat erin stond.

* Alle organisaties laten bij het opstellen hun e-mailconventie juridisch tegen het licht houden.

* De ondernemingsraad wordt meestal betrokken bij het opstellen, maar de ondernemingsraad bij één organisatie vond dit niet nodig, aangezien er naar zijn mening niets nieuws in de conventie zou staan.

* De communicatie van de conventie richting werknemers gebeurt meestal verre van optimaal. Zoals gezegd, kenden de geïnterviewde gebruikers de conventie bijna allemaal, maar vertelden zij ook dat veel van hun collega's de conventie nauwelijks blijken te kennen.

* Bij alle organisaties was een gestructureerde aanpak aanwezig om met e-mailincidenten om te gaan. Vaak is dit een algemene aanpak die niet specifiek voor alleen e-mailincidenten wordt gebruikt.

* De officiële richtlijnen bij alle organisaties met een e-mailconventie zijn dat deze periodiek wordt herzien en zo nodig wordt aangepast. Er werd wel toegegeven dat er meestal wat slordig wordt omgesprongen met deze richtlijnen en het herzien niet altijd op het voorgeschreven tijdstip gebeurt.

Deze resultaten zijn gebruikt voor het samenstellen van de ontwikkelfasering die in de volgende paragraaf wordt beschreven.

Ontwikkelfasering

Structuur en aanpak

Op basis van de theorie en het praktijkonderzoek heeft KPMG een ontwikkelfasering voor e-mailconventies ontwikkeld, die is afgebeeld in figuur 1.

De aanpak kenmerkt zich door vier fasen. De eerste drie fasen zijn de ontwikkelfasen, namelijk Voorbereiding, Inhoudsbepaling en Invoering. De vierde fase is het daadwerkelijke Gebruik van de e-mailconventie. De fasen moeten bij voorkeur opeenvolgend worden doorlopen. Binnen de fasen is er geen vaststaande volgorde van activiteiten. Uitzondering is het bepalen van technische beveiligingsmaatregelen. Dit kan het beste worden gedaan vóór het opstellen van de conventie, omdat de maatregelen mogelijk moeten worden vermeld in de conventie.

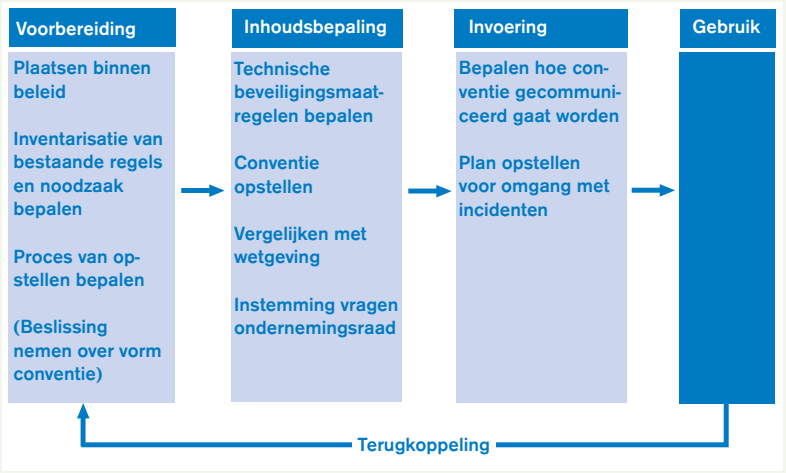
Voorbereiding

De eerste fase omvat:
* plaatsen binnen beleid;
* inventarisatie van bestaande regels en noodzaak bepalen;
* proces van opstellen bepalen;
* (beslissing nemen over vorm conventie).

Bij de voorbereiding wordt er gekeken binnen welk beleid de e-mailconventie ontwikkeld gaat worden. Verder wordt de bestaande regelgeving geïnventariseerd en wordt bepaald of een e-mailconventie wel nodig is. Hierbij moet worden gekeken naar de mogelijke impact van bedreigingen van e-mail voor de organisatie en naar de cultuur van de organisatie. Vragen die men hierbij kan stellen, zijn: Past een conventie wel in deze cultuur? Zijn er niet andere regelingen of grondwaarden die al genoeg houvast bieden?

In de praktijk blijkt dat een e-mailconventie beleidsmatig het beste kan worden geplaatst zoals in figuur 2 is weergegeven. Uiteindelijk zal de e-mailconventie altijd vallen onder het beleid voor goed gebruik van IT-middelen door werknemers. Dit beleid is onderdeel van het beleid voor informatiebeveiliging, dat weer een onderdeel is van het algemeen beveiligingsbeleid en het informatie/IT-beleid van de organisatie.

In de activiteit 'proces van opstellen bepalen' moet worden nagedacht over wie de conventie gaat opstellen. Dit zal vaak de initiatiefnemer zijn, een persoon of afdeling die verantwoordelijk is voor informatiebeveiliging binnen de organisatie. Ook als de initiatiefnemer iemand anders is, bijvoorbeeld de leiding van de organisatie, moeten zij degenen zijn die hiermee aan de slag gaan. Ook moet tijdens deze activiteit worden nagedacht over wie bij het proces gaan worden betrokken. De directie of Raad van Bestuur moet altijd vertegenwoordigd zijn. Soms is dit al vastgelegd in een standaardprocedure in de organisatie. Het kan verstandig zijn om deze standaardprocedure goed tegen het licht te houden om vast te stellen of deze bij het opstellen van de e-mailconventie ook voldoet. Een speciaal team samenstellen om de conventie te becommentariëren met daarin vertegenwoordigers van verschillende partijen uit de organisatie kan ook, maar is niet de enige mogelijkheid.



Figuur 1. KPMG-ontwikkelfasering voor e-mailconventies.

Het bepalen van de vorm van de conventie staat tussen haakjes, want dit is geen activiteit die noodzakelijkerwijs in deze fase wordt uitgevoerd. Een andere mogelijkheid is om de beslissing over de vorm te integreren met het communicatieplan in de fase Invoering. Ook kan het zo zijn dat deze beslissing al bij de eerste activiteit tijdens het noodzakelijkheidsonderzoek wordt genomen.

Inhoudsbepaling

De tweede fase omvat:
* technische beveiligingsmaatregelen bepalen;
* conventie opstellen;
* vergelijken met wetgeving;
* instemming vragen ondernemingsraad.

Bij het bepalen en becommentariëren van de technische beveiligingsmaatregelen en de inhoud van de conventie zijn er twee belangrijke overwegingen:
1. Welke nadelen van e-mail kunnen een bedreiging vormen voor de organisatie?
2. Wat botst niet met de organisatiecultuur en zal de mogelijkheden die e-mail voor de organisatie heeft niet te veel beperken?

Het structureel op inhoud scannen van e-mails van werknemers behoeft extra toelichting, omdat dit privacygevoelig is. Bij de overweging om dit te doen, worden allereerst de twee bovenstaande overwegingen meegenomen, dus de nadelen en de organisatiecultuur. Ook wordt er gekeken naar de proportionaliteit en de subsidiariteit, ofwel is het middel evenredig ten opzichte van het doel en is er geen minder vergaande methode die vol-

Figuur 2. Beleidsmatige plaatsing van e-mailconventies.

Drs. W.J.P. van de Meent is werkzaam bij KPMG Information Risk Management in Amstelveen. Zijn expertisegebieden betreffen de advisering over e-business in het algemeen en de beveiligingsaspecten van e-business in het bijzonder. Hiervoor studeerde hij Bestuurlijke Informatiekunde aan de Katholieke Universiteit Brabant in Tilburg. Zijn afstudeeronderzoek voor deze studie, welke hij uitvoerde in opdracht van het Platform Informatiebeveiliging, heeft de basis gelegd voor dit artikel.

doet. Er zou bijvoorbeeld alleen kunnen worden gescand in het geval er een vermoeden is van misbruik. Verder moet worden voldaan aan de volgende voorwaarden:

1. Er moet zorgvuldig worden gescand en een goede functiescheiding is noodzakelijk.
2. De ondernemingsraad heeft met de maatregel ingestemd.
3. Er is hierover duidelijk gecommuniceerd richting werknemers.
4. De werknemers hebben inzage-, correctie- en verzetsrecht op de over hen verzamelde gegevens.

Invoering

De derde fase omvat:

* bepalen hoe conventie gecommuniceerd gaat worden;
* plan opstellen voor omgang met incidenten.

Bij de communicatie van de conventie richting de werknemers moet er op zoveel mogelijk manieren voor worden gezorgd dat alle werknemers waar de conventie relevant voor is, de conventie kennen en weten dat ze zich hieraan moeten houden. Ook moeten ze begrijpen dat de conventie nuttig en zinvol is, dus het doel van de conventie moet ook duidelijk worden gecommuniceerd. Tevens moeten ze het idee hebben dat de leiding van de organisatie de conventie ondersteunt. Beveiliging kan een ondergeschoven kindje zijn, omdat het nut hiervan pas blijkt als er iets ergs gebeurt. Sommige organisaties hebben een standaardprocedure voor het communiceren van dit soort regelingen, maar deze heeft niet altijd het gewenste effect. Deze procedure moet eventueel worden veranderd of de communicatie moet via andere kanalen gebeuren. Mogelijke manieren zijn het opsturen van de conventie naar de huisadressen van alle medewerkers, het zorgen voor trainingen en opleidingen en het opnemen van de conventie in de arbeidsvoorwaarden.

> Een e-mailconventie moet vanwege de snel veranderende technologieën en mogelijkheden regelmatig tegen het licht worden gehouden.

Voor het afhandelen van incidenten is een speciaal incidententeam niet noodzakelijk, wel is het van belang dat een organisatie heeft bepaald hoe ze met incidenten omgaat. Vaak is dit een standaardprocedure en staat dit ook in de CAO/arbeidsvoorwaarden. Hierbij kunnen ook een ondernemingsraad en afdeling Juridische Zaken worden betrokken. Er moet altijd worden geprobeerd te achterhalen hoe een bepaald incident tot stand is gekomen. Zo kan er worden voorkomen dat er te lichte of te zware sancties worden opgelegd.

Gebruik

Na invoering kan de e-mailconventie in gebruik worden genomen.

Terugkoppeling

Vanwege de snel veranderende technologieën en mogelijkheden die e-mail heeft, moet de conventie regelmatig tegen het licht worden gehouden. Dit houdt in principe in, dat de activiteit van het inventariseren van bestaande regels en het bepalen van de noodzakelijkheid opnieuw moet worden uitgevoerd. Alleen zijn de bestaande regels nu de huidige conventie en moet worden bepaald of het noodzakelijk is dat deze wordt aangepast. Als dat het geval blijkt, kan de fasering weer worden doorlopen, of de relevante activiteiten daarvan.

Conclusie

E-mail brengt een aantal nadelen met zich mee. De gevolgen van deze nadelen proberen te beperken door technische beveiligingsmaatregelen is meestal niet afdoende. Vaak is het beter te proberen het gedrag van de werknemers te verbeteren door middel van een e-mailconventie. De technische maatregelen dienen hier een aanvulling op te zijn. Het ontwikkelen van een e-mailconventie die maximaal effect sorteert, is niet eenvoudig. De ontwikkelfasering voor e-mailconventies, die in dit artikel is toegelicht, kan worden gebruikt als kader voor de aanpak van deze activiteit.

Literatuur

[Brow99]
J. Browning, *Monitoring E-mail: A Necessary Evil*, Gartner Group, Research Note Tactical Guidelines, 2 August 1999.

[Gask98]
J.E. Gaskin, *Internet acceptable usage policies: Writing and implementation*, Information Systems Management, Spring 1998, p. 20-25.

[Hind99]
S. Hinde, *E-mail Can Seriously Damage Your Health*, Computers & Security, 18, 5, 1999, p. 396-408.

[Hoof98]
B. van den Hooff, *E-mail in bedrijf: effecten en beheer van elektronische communicatie in organisaties*, Management & Informatie, 6, 5, 1998, p. 4-11.

[Luca98]
W. Lucas, *Effects of E-mail on the organization*, European Management Journal, 16, 1, 1998, p. 18-30.

[Nelm99]
C. Nelms, *Internet E-mail Risks and Concerns*, Computers & Security, 18, 5, 1999, p. 409-418.

[Regi01]
Registratiekamer, *Goed werken in netwerken – Regels voor controle op e-mail en internetgebruik van werknemers*, http://www.registratiekamer.nl/bis/top-1-1-9.html, 2001.

[Spro91]
L. Sproull en S. Kiesler, *Connections; new ways of working in the networked organization*, MIT Press, Cambridge, Mass., 1991.

[Walt92]
J.B. Walther, *Interpersonal Effects in Computer Mediated Interaction: A Relational Perspective*, Communication Research, February, 19(1), 1992, p. 52-90.

Bijlage: Publicatie Registratiekamer

Niet in het onderzoek meegenomen, maar wel relevant voor dit onderwerp is de publicatie die de Registratiekamer eind 2000 gedaan heeft met de titel *Goed werken in netwerken – Regels voor controle op e-mail en internetgebruik van werknemers*. Deze publicatie adviseert werkgevers over de controle op e-mail en internetgebruik van werknemers. De publicatie sluit af met een beknopt overzicht van de vuistregels voor werkgevers. Voor de volledigheid van dit artikel worden deze vuistregels hierna genoemd.

Algemeen

1. Behandel zaken on line op dezelfde manier als zaken off line.
2. Stel heldere regels op met de instemming van de ondernemingsraad.
3. Publiceer de regels op een voor de werknemer toegankelijke wijze.
4. Stel vast in hoeverre privé-gebruik van de faciliteiten is toegestaan, en welke software daarvoor mag worden gebruikt.
5. Maak verboden gebruik voorzover dat kan softwarematig onmogelijk.
6. Anonimiseer rapportages en gebruiksstatistieken.
7. Houd rekening met de back-ups van het systeem.
8. Garandeer de integriteit van de systeembeheerder.
9. Bespreek geconstateerd gedrag zo spoedig mogelijk met betrokkene.
10. Bied inzage in de gegevens.
11. Evalueer de regels periodiek.

E-mail/internet

12. Zorg voor een scheiding in zakelijke mail en privé-mail. Als dat niet kan, ontzie privé-mail dan zoveel mogelijk.
13. Beperk de controle tot het vooraf geformuleerde doel.
    Voorzie in op de doeleinden toegesneden controlemechanismen.
    Doeleinden kunnen zijn:
    - begeleiding/individuele beoordeling;
    - bewijs/archief;
    - systeem- en netwerkbeveiliging;
    - controle op bedrijfsgeheimen;
    - voorkomen van negatieve publiciteit;
    - tegengaan van seksuele intimidatie;
    - naleving afspraken over verboden gebruik;
    - kosten- en capaciteitsbeheersing.
14. Voer de controles op naleving zo beperkt mogelijk uit (maatwerk).
15. Beperk de logging van het netwerkgebruik tot de verkeersgegevens (e-mail) of de gegevens die noodzakelijk zijn voor het doel (internet).
16. Bewaar de loggegevens niet langer dan noodzakelijk is:
    - e-mail: 1 maand;
    - internet: 1 maand.
17. Ontzie geprivilegieerde informatie van ondernemingsraadleden en bedrijfsartsen in elektronische berichten.