

Waarom het nodig is om e-mails te archiveren

Waarom het van belang is om zakelijke e-mails te archiveren

Hoewel het gebruik van e-mail en Instant Messaging in organisaties steeds verder toeneemt, wordt er nog steeds gedebatteerd over het bewaren van dergelijke elektronische correspondentie. Dit white paper gaat in op deze onzekerheden en legt uit waarom e-mailarchivering een integraal onderdeel zou moeten zijn van iedere organisatie. Daarnaast wordt ingegaan op de diverse methoden voor het installeren en beheren van archiveringsoplossingen in organisaties en de belangrijkste eisen waaraan een goed archiveringssysteem moet voldoen.

Inleiding

In een recent onderzoek vroeg SERVO 100 van zijn beste klanten naar hun doelstellingen voor 2005. E-mailarchivering staat in de top 5 van zakelijke prioriteiten voor dit jaar. Dit is tevens zichtbaar in de markttrends die laten zien dat de vraag naar producten voor e-mailarchivering verzesvoudigd is. Dit white paper bespreekt waarom e-mailarchivering belangrijk is.

Inleiding	2
De rol van e-mail in het bedrijfsleven	2
Wat betekent e-mailarchivering?	2
Wat zijn de belangrijkste redenen om e-mail te archiveren?	3
Installatie en beheer van archiveringsproducten.....	7
Over welke functies moet een e-mailarchiveringproduct beschikken?	8
Over GFI MailArchiver	9
Over GFI	10
Referenties	11

De rol van e-mail in het bedrijfsleven

De laatste vier jaar is e-mail het belangrijkste communicatiemiddel geworden in bedrijven. E-mail biedt bedrijven een snelle methode voor het verzenden van onder andere kooporders, offertes en verkooptransacties waar ook ter wereld met zo min mogelijk moeite. Uit onderzoek van marktonderzoeksbureau Gartner Group is gebleken dat bijna 97% van de zakelijke communicatie via e-mail plaatsvindt. Bovendien blijkt uit onderzoek van Osterman Research dat e-mail nu in 79% van de organisaties geaccepteerd wordt als schriftelijke bevestiging van bestellingen.

Aangezien e-mails de elektronische vervangers van juridische bedrijfsinformatie zijn geworden, vormt de informatie die via deze elektronische correspondentie wordt uitgewisseld een archief. Dergelijke correspondentie moet dus gedurende een bepaalde periode worden bewaard. Dit is vaak vastgelegd in statuten. Omdat e-mail zo populair is geworden in het bedrijfsleven, zijn diverse wetten ingevoerd om privacy te beschermen, standaarden voor corporate governance op te leggen en voor ethisch gedrag te zorgen. Enkele voorbeelden zijn de Sarbanes-Oxley Act (SOX), de Gramm-Leach Bliley act (GLBA) en de Freedom of information act (FOIA).

Wat betekent e-mailarchivering?

Een e-mailarchief is een veilige opbergplaats waar u uw e-mail kunt bewaren voor juridische en operationele doeleinden. Een goed e-mailarchiveringssysteem haalt automatisch de inhoud en bijlagen uit inkomende en uitgaande berichten en slaat ze na indexering op in alleen-lezenformaat. Op deze manier bent u er zeker van dat gearchiveerde berichten in hun

oorspronkelijke staat worden bewaard.

Met e-mailarchivering reduceert u het aantal online e-mails op de mailserver en dus de vraag naar opslagruimte. Bovendien nemen e-mailarchieven minder opslagruimte in beslag dan andere methoden voor e-mailopslag.

De actieve benadering van e-mailarchiveringsoplossingen zorgt ervoor dat het bedrijf een gecentraliseerde en toegankelijke kopie van alle e-mail heeft. Dit biedt extra bescherming tegen verwijdering van e-mails door eindgebruikers. E-mailarchivering elimineert ook de noodzaak om op elke individuele computer naar persoonlijke archieven te zoeken.

Uit onderzoek van Osterman Research blijkt dat 46% van de bedrijven tape backups gebruikt om e-mails te 'archiveren'. Backups en archiveringssystemen hebben verschillende doelen. Backups dienen om kopiën van data op te slaan voor het geval dat het origineel verloren raakt. Archieven beschermen data zodat ze kunnen worden geraadpleegd wanneer dat nodig is. De kosten van het zoeken naar elektronische records wanneer inzage van stukken nodig is kunnen astronomisch zijn: er kunnen maanden voor nodig zijn om de backup tapes te doorzoeken. E-mailarchiveringssystemen bieden geavanceerde zoek- en terughaalfuncties. Op deze manier kunnen gebruikers hun berichten terugvinden op een snelle en efficiënte manier. Zonder effectief e-mailarchiveringssysteem is het zoeken naar een email record moeilijker dan het zoeken naar een speld in een hooiberg. In de zaak Murphy Oil USA vs. Flour Daniel heeft de gedaagde de e-mails uit 93 tape backups moeten herstellen en printen. De kosten bedroegen \$6,2 miljoen.

E-mailarchiveringsoplossingen stellen beheerders in staat om toegangsbeperkingen in te stellen. Deze beperkingen zorgen voor bescherming van intellectueel eigendom en ook voor integriteit van data en voor vertrouwelijkheid in overeenstemming met de statuten.

Wat zijn de belangrijkste redenen om e-mail te archiveren?

Er zijn vier hoofdredenen voor het archiveren van zakelijke e-mail. Dit zijn naleving van wetgeving en voorschriften, procesvoering, opslagbeheer en kennisbeheer.

Naleving van wetgeving en voorschriften

Toezichthoudende instanties hebben ervoor gezorgd dat de vraag naar e-mailarchiveringsproducten is toegenomen. Naar schatting zijn er wereldwijd meer dan 10.000 reguleringen ingevoerd. Organisaties worden door striktere controles and strengere straffen gedwongen om wetten en voorschriften serieuzer te nemen. In maart 2004 heeft de Bank of America een boete van \$10 miljoen gekregen omdat e-mails niet lang genoeg waren bewaard en de door de Securities and Exchange Commission (SEC) opgevraagde informatie niet op tijd was verstrekt.

Hoewel de data die onder de regelingen vallen per sector verschillen, moeten alle records die met de bedrijfsactiviteit van een organisatie te maken hebben, voldoen aan wettelijke eisen en voorschriften. Hieronder vallen onder andere gegevens betreffende werknemers en klanten, correspondentie tussen organisaties en financiële documentatie. Zo is de Sarbanes-Oxley Act (SOX) van invloed op alle sectoren en staan er zware straffen op het opzettelijk wijzigen of verwijderen van documenten om derde partijen te bedriegen. Dit betekent dat controleurs documenten minimaal vijf jaar moeten bewaren vanaf het einde van het fiscale jaar. Hoewel het een Amerikaanse wet is, is SOX ook van toepassing op Europese bedrijven die in Amerika op de beurs genoteerd staan en bedrijven die zaken doen met de VS. Zie <http://www.s-ox.com/> voor meer informatie over Sarbanes-Oxley.

Andere wetgevingen stellen eisen aan specifieke gereguleerde sectoren. Zo zijn de Securities and Exchange Commission (SEC) en National Association of Securities Dealers (NASD) twee reguleerders die over de financiële wereld gaan. SEC Rules 17a-3/a-4 and NASD Rules 3010/3110 verplichten effectenmakelaars en dealers om alle e-mails met betrekking op hun handelsactiviteiten minimaal zes jaar te bewaren. Bovendien moet deze documentatie de eerste twee jaar in een geïndexeerde en eenvoudig toegankelijke opslag worden bewaard. Deutsche Bank Securities Inc., Goldman Sachs & Co., Morgan Stanley, Solomon Smith Barney Inc. en U.S. Bancorp Piper Jaffray Inc hebben elk een boete van \$1,65 miljoen opgelegd gekregen omdat ze niet aan SEC Rule 17a-4 voldeden en niet in staat bleken om de in een onderzoek opgevraagde e-mails te produceren. Zie <http://www.sec.gov/> en <http://www.nasd.com/> voor meer informatie over SEC en NASD.

Een andere sterk gereguleerde sector is de gezondheidszorg. De Health Insurance Portability Accountability Act (HIPAA) dekt alle soorten papieren en elektronische records met persoonlijke informatie en details die relevant zijn voor de medische geschiedenis van een individu. Deze informatie staat bekend als Protected Health Information (PHI). Hoewel maar weinig e-mails dit soort informatie bevatten, moeten alle organisaties deze informatie beheren in overeenstemming met HIPAA-reguleringen. Firma's die aan HIPAA-reguleringen moeten voldoen zijn zorgverleners, ziektekostenverzekeringen, verrekeningsbureaus voor de gezondheidszorg en werkgevers die zorg verlenen. Medische gegevens moeten tussen de vijf en zes jaar bewaard worden. Volgens bepaalde statuten moet dergelijke documentatie echter bewaard worden tot twee jaar na de dood van de patiënt. Kijk voor meer informatie over HIPAA op <http://www.hipaa.com/>.

De Food and Drug Administration (FDA) is de toezichthoudende instantie die in de VS toezicht houdt op firma's die medicijnen, medische apparatuur, cosmetica en voeding fabriceren. De reguleringen die in deze sectoren het beheer van gegevens bepalen staan bekend als GxP. Meer informatie over de FDA en diens reguleringen is te vinden op <http://www.fda.gov/>.

Ook overheidsinstanties moeten e-mails archiveren. Zij moeten voldoen aan de eisen van de Freedom of Information Act (FOIA), de Patriot Act, National Archive Records Administration (NARA) en andere wetten. Kijk voor meer informatie op <http://www.usgs.gov/foia/> en

<http://www.archives.gov/>.

Hoewel er vele verschillende reguleringen bestaan die elk hun eigen regels lijken te hebben, is naleving van wetgeving en voorschriften gebaseerd op drie concepten:

1. Behoud – Data moeten in originele staat worden bewaard zonder dat ze gewijzigd of verwijderd worden.
2. Beveiliging – De data moeten beschermd worden tegen alle mogelijke dreigingen, waaronder toegang door onbevoegden en alles waardoor de informatie beschadigd of onbeschikbaar zou kunnen worden.
3. Controleerbaarheid – De informatie moet goed beschermd zijn en toch gemakkelijk en snel toegankelijk zijn voor geautoriseerd personeel wanneer nodig.

Niet alle e-mail valt onder deze regels. Uitzonderingen zijn bijvoorbeeld spam, die uiteraard niet bewaard hoeft te worden, en persoonlijke e-mails, hoewel de laatste wel tijdens onderzoeken kunnen worden opgevraagd als bewijsmateriaal.

Litigation support

Bijna elk bedrijf krijgt vroeg of laat te maken met rechtszaken. Inzage van stukken is het proces waarbij de bij een rechtszaak betrokken partijen door de rechtbank worden verzocht om informatie in te dienen die relevant is voor de zaak. Het bedrijf dat dit verzoek krijgt, is verplicht om zijn archieven te doorzoeken en alle relevante/opgevraagde informatie tijdig in te dienen. Het produceren van deze informatie kan zeer kostbaar zijn. Vaak zijn de kosten zelfs hoger dan de schadevergoeding die in de rechtszaak wordt geëist. Dit geldt vooral voor organisaties die niet over een adequaat e-mailarchiveringsproduct beschikken. Zo bedroegen de kosten van het herstel van 77 tape backups in de zaak Zubulake vs. Warburg (USB Bank) \$165.954 en de kosten van het doorzoeken van deze backups \$107.694.

Een probleem met dergelijke verzoeken is het feit dat er geen limiet is op hoever een bedrijf terug in de tijd moet zoeken. Organisaties moeten alle relevante e-mails kunnen overleggen, ongeacht hoe oud deze berichten zijn. De mate van volledigheid en beschikbaarheid van de opgevraagde informatie en de benodigde tijd om deze informatie op te zoeken zijn afhankelijk van hoe het bedrijf de opslag van e-mails beheert. Elektronische documentatie kan op vele plaatsen en media worden opgeslagen, waaronder mailservers, PST-bestanden op desktops, laptops, PDA's, backup tapes en andere draagbare media. E-mails die lokaal zijn opgeslagen, bijvoorbeeld op de harde schijf of PDA van een werknemer, zijn zelden nuttig voor werkgevers. Het doorzoeken van iedere computer in het bedrijf is niet alleen kostbaar, maar houdt ook risico in op het gebied van beveiliging en intellectueel eigendom. Bovendien weten IT-medewerkers vaak niet van het bestaan van informatie die door eindgebruikers is opgeslagen en wordt deze informatie dus niet opgemerkt. Wanneer e-mail niet in een daadwerkelijk (en centraal) archief is opgeslagen, kost het herstellen ervan enorm veel tijd en geld (vaak meer dan \$25.000). Het

bedrijf dat de informatie levert, moet de kosten ervan betalen. Deze kosten kunnen niet worden teruggevorderd.

De informatie moet accuraat, compleet en indien mogelijk in oorspronkelijke staat zijn. Aangezien back-upsystemen niet volmaakt zijn, kunnen data verloren gaan of vernietigd worden. Bedrijven die er niet in slagen de opgevraagde informatie te overleggen kunnen schuldig bevonden worden aan onrechtmatige vernietiging van bewijsmateriaal. Hieronder valt onder andere het verwijderen van e-mails. Dergelijke omstandigheden kunnen ertoe leiden dat de rechtbank ervan uitgaat dat de verloren gegevens nadelig waren voor de partij die er niet in is geslaagd om deze te overleggen. Dit was het geval in de zaak Zubulake vs USB AG bank. Toen de bank er niet in slaagde het benodigde bewijs te leveren, instrueerde rechter Shira Scheindlin de jury te concluderen dat het niet-geleverde bewijs nadelig was voor de bank. Ook kan het vernietigen van bewijsmateriaal tot hoge boetes leiden. Zo heeft Philip Morris International, één van de grootste tabaksbedrijven ter wereld, \$2,75 miljoen moeten betalen omdat het bedrijf e-mails had vernietigd.

Opslagbeheer

De vereiste opslagruimte voor e-mails neemt steeds verder toe. Naar schatting heeft één op de vier organisaties te maken met een groei van meer dan 25% per jaar. Deze drastische groei wordt voornamelijk veroorzaakt door toegenomen gebruik van e-mail en toegenomen gebruik van attachments waardoor de omvang van de gemiddelde e-mail is gestegen van 22 KB naar 350 KB. Naar schatting heeft bijna 50% van de organisaties meer dan 150 MB aan opslagruimte per gebruiker. Organisaties maken vaak gebruik van opslagquota om te voorkomen dat e-mails zoveel ruimte in beslag nemen dat de server slechter gaat presteren. Het nadeel van quota is dat de productiviteit van eindgebruikers omlaag gaat. Nog afgezien van het feit dat gebruikers hun mail niet meer kunnen gebruiken als ze de limiet hebben bereikt, kan het gebruik van quota zeer ernstige gevolgen hebben. Zo kan het gebeuren dat gebruikers na het bereiken van hun limiet belangrijke berichten verwijderen om ruimte te creëren voor nieuwe mail.

De toename van e-mailgebruik en de relatieve toename van de omvang van e-mails heeft ook invloed op de efficiëntie, betrouwbaarheid en snelheid van servers. Volgens onderzoek van Osterman Research neemt de opslag van e-mail elk jaar met 37% toe. 'Live' (online) opslag van e-mail vereist dus meer fysieke opslagruimte en betere hardware.

Wetten en voorschriften hebben verder bijgedragen aan de toegenomen vraag naar opslagruimte door organisaties te verplichten om oude e-mails een bepaald aantal jaren te bewaren.

Hoewel het mogelijk is om opslagproducten te gebruiken om met dit probleem om te gaan, biedt een product voor e-mailarchivering een veelzijdiger oplossing. Een efficiënt archiveringsproduct centraliseert uw e-mailrecords niet alleen, maar slaat de e-mails op in gecomprimeerd formaat, zodat u een aanzienlijke hoeveelheid schijfruimte bespaart vergeleken

met traditionele opslag van e-mail. Bovendien worden de e-mails automatisch gearchiveerd zodra ze door de message store gaan. Gebruikers kunnen hun mailbox dus opschonen zonder dat ze belangrijke berichten kwijt kunnen raken. Bovendien zal een archiveringsproduct dat geautoriseerde gebruikers in staat stelt e-mails vanuit een centrale opslagruimte te bekijken, hen aanmoedigen om dit ook te doen. Lokaal opgeslagen PST-bestanden worden dan overbodig. Aangezien PST-bestanden meestal 2 tot 5 keer zoveel ruimte in beslag nemen als een e-mailarchief, leidt dit tot een aanzienlijke besparing van schijfruimte.

Kennisbeheer

Het e-mailsysteem van een organisatie is een opslagplaats van kennis. Het kan enorm veel informatie bevatten die vaak van levensbelang is voor het bedrijf. Toegang tot deze informatie kan ervoor zorgen dat gebruikers productiever worden.

Een archiveringssysteem kan de juiste knowledge management tools bieden (zoals het sorteren van e-mailrecords en geavanceerde zoekfuncties) om IT-medewerkers en eindgebruikers in staat te stellen de kennis die in het e-mailarchief ligt opgeslagen, te beheren.

Installatie en beheer van archiveringsproducten

Er zijn twee methoden voor het installeren en beheren van e-mailarchiveringsoplossingen:

- Volledig in-house
- Een gehoste oplossing waarbij het archief wordt beheerd in het datacentrum van een derde partij.

Bij een in-house oplossing staat uw e-mailopslagruimte op een server in het kantoorgebouw. Het grootste voordeel hiervan is dat vertrouwelijke informatie achter de firewall ligt opgeslagen en door het eigen personeel wordt beheerd. Hierdoor bent u verzekerd van betere controle over integriteit en vertrouwelijkheid. In dit geval gebruikt de organisatie alleen haar eigen hulpbronnen en is er dus continu zicht op in welke mate de wetgeving wordt nageleefd. De belangrijkste nadelen zijn de kosten en de plotselinge impact op uw IT-afdeling. Om een intern e-mailarchief te kunnen installeren, moet het bedrijf een adequaat e-mailarchiveringsprogramma en een server aanschaffen.

Gehoste oplossingen kosten vooraf minder geld dan in-house oplossingen. Het product kan vrijwel meteen gebruikt worden zonder dat er geïnvesteerd hoeft te worden in hardware en IT-medewerkers. Ook de lopende kosten zijn laag. Nieuwe functionaliteiten en upgrades worden immers geïmplementeerd door de provider. Bij gehoste oplossingen worden de berichten opgevangen door een softwareapplicatie op de mailserver en worden ze vervolgens via internet naar een opslagruimte van een derde partij gestuurd om aldaar te worden gearchiveerd. Geautoriseerde gebruikers kunnen vervolgens toegang tot de data verkrijgen met behulp van een webbrowser of een compatibele e-mailclient.

Uit onderzoek van Osterman Research blijkt echter dat bijna 70% van de organisaties de voorkeur geeft aan een oplossing in-house. Dit komt vooral door het feit dat organisaties niet graag op een derde partij vertrouwen als het gaat om het opslaan van vertrouwelijke gegevens. Bovendien kunnen bedrijven die hun eigen e-mailsystemen beheren zelf bepalen wat wanneer wordt gedaan. Bij een gehost systeem concurreren de prioriteiten van het bedrijf met die van de service provider. Een dergelijke beperking kan tot een verhoogd risico leiden: het kan gebeuren dat records niet compleet zijn en/of niet op tijd gevonden kunnen worden. Ook moeten organisaties rekening houden met de mogelijkheid dat de provider failliet gaat of er niet in slaagt een adequate service te leveren. In dat geval zal men gedwongen zijn om van provider te veranderen of over te schakelen naar een in-house oplossing. In beide gevallen wordt de archiveringsdienst ontregeld en moet er extra geld worden uitgegeven.

Sommige organisaties zien gehoste archiveringsoplossingen als een manier om de verantwoordelijkheid af te schuiven op een ander. Dit is echter een misvatting: de verantwoordelijkheid ligt nog steeds bij de eigenaar van de data.

Over welke functies moet een e-mailarchiveringsproduct beschikken?

- **Minimale interventie door gebruikers** – Berichten moeten automatisch worden gearchiveerd, met zo min mogelijk interventie door gebruikers.
- **Indexering van records en zoekfunctionaliteiten** – Gearchiveerde e-mails (en vooral de inhoud daarvan) moeten worden geïndexeerd zodat records snel gevonden kunnen worden.
- **Beleid voor het behoud van data** – Het systeem moet beschikken over configuratiefuncties waarmee het bedrijf archiveringscriteria kan definiëren. Deze functies moeten in ieder geval zorgen voor de archivering van specifieke mailboxen en berichten van specifieke domeinen of e-mailadressen. Op deze manier worden spam en andere informele correspondentie automatisch uitgesloten van archivering.
- **Zekerheid en knoeibestendigheid** – Een archiveringssysteem moet records kunnen beschermen tegen verlies, beschadiging en misbruik. Authenticiteit van records (behoud van records in hun oorspronkelijke staat) is één van de belangrijkste eisen in vele wettelijke voorschriften. Bovendien moeten archiveringsprogramma's over functies beschikken waarmee de toegang beperkt kan worden.
- **Toegang tot archieven voor eindgebruikers en management** – Met deze functie kunnen bedrijven hun e-mailarchief gebruiken als centrale kennisopslagplaats waar geautoriseerde gebruikers informatie uit kunnen halen. Een ander voordeel is dat geautoriseerde gebruikers zoals toezichthouders bij de informatie in het archief kunnen zonder dat ze

daarvoor de hulp van IT-medewerkers hoeven in te roepen.

- **Ondersteuning van verschillende berichtenplatforms** – Het archiveringssysteem ondersteunt alle grote berichtenplatforms zodat compatibiliteit gegarandeerd is.

Over GFI MailArchiver

GFI MailArchiver for Exchange is een gebruiksvriendelijke oplossing voor het archiveren van al uw interne en externe e-mail in één of meer SQL-databases. Zo heeft u geen gedoe meer met PST-bestanden. Gebruikers kunnen via een webgebaseerde interface hun oude e-mails gemakkelijk terugvinden. Bovendien kunnen ze hun e-mails snel uit het archief terughalen dankzij de OneClick Restore-functie. GFI MailArchiver maakt het voldoen aan wettelijke voorschriften (zoals de Sarbanes-Oxley Act) heel eenvoudig. GFI MailArchiver for Exchange maakt gebruik van de logboekfunctionaliteit van de Exchange Server 2000/2003 en is daardoor zeer schaalbaar en betrouwbaar voor een concurrerende prijs. U kunt meer informatie en een gratis trialversie downloaden op <http://www.gfi.nl/nl/mar/>.

Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide, Hamburg en Cyprus die wereldwijd meer dan 160.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

Referenties

Osterman Research - <http://www.ostermanresearch.com/>.

Messaging archiving Market Trends, 2005-2008.

How to Evaluate and Choose a Messaging archiving Solution.

Sarbanes-Oxley Compliance Journal - <http://www.s-ox.com/>.

Compliance Pipeline - <http://www.compliancepipeline.com/>.

Transform Magazine - <http://www.transformmag.com/compliance/>.

U.S. Securities and Exchange Commission - <http://www.sec.gov/>.

National Association of Securities Dealers (NASD) - <http://www.nasd.com/>.

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.