Hou het veilig!

Door gebruik te maken van e-HR win je heel wat tijd en kun je efficiënter zijn. Maar elektronica en software zijn niet onfeilbaar, en daarom moet je de nodige maatregelen nemen om je gevoelige HR-informatie te beschermen. In tien praktische vragen gaan we dieper in op beveiliging, vertrouwelijkheid en hoe HR, en ook de werknemers, op de juiste manier moeten omgaan met de huidige technologie. Over mailpolicies, privacy, confidentialiteit en hackers... Wat een wereld!

TEKST: ANNICK CLAUS

Welke toon hanteer ik in een e-mail?

Een smiley hier, een grapje of afkorting daar. Hoewel bij e-mails alles zwart op wit staat, wordt er bijzonder informeel mee omgegaan. Daarin schuilt dan ook een groot gevaar, want alles wat je schrijft, wordt bewaard. Bovendien wordt e-mail zo frequent gebruikt, dat je makkelijk te los omgaat met collega's, werknemers of klanten. Je houdt het best formeel.

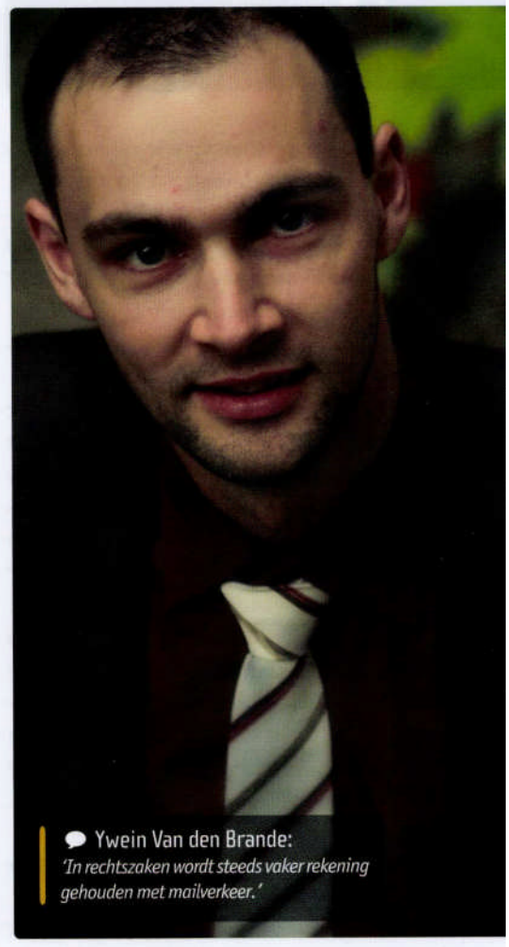
'In rechtszaken wordt steeds vaker rekening gehouden met mailverkeer', merkt Ywein Van den Brande, advocaat bij De Bandt, Keustermans & Van den Brande, op. *'Berichten worden vaak geschreven en verstuurd in een emotionele opwelling, en sommige e-mails kunnen later wel eens beschouwd worden als een bekentenis. De bewuste e-mails verwijderen, heeft meestal geen zin. In het kader van een straf- of mededingingsonderzoek kunnen experts ze toch terugvinden. Een handgeschreven kattebelletje verdwijnt daarentegen in de prullenmand en duikt in de meeste gevallen niet meer op.'*

Ben ik zeker van de identiteit van de verzender?

Dat iemands naam onder een e-mail staat, bewijst nog niet dat hij of zij ook de verzender is. Andersom zal ook jij in een conflict moeten bewijzen dat jij die mail echt verzonden hebt en dat de inhoud niet gewijzigd werd. Bij erg belangrijke e-mails maak je daarom best gebruik van een gekwalificeerde elektronische handtekening. Die is op een veilige manier aangemaakt en wordt geleverd met een certificaat door een erkende dienstverlener, zoals Certipost of de Belgische overheid (eID). Een rechter mag de authenticiteit en integriteit van een e-mail met een dergelijke handtekening dan ook niet in twijfel trekken. Met andere woorden, een e-mail of document dat op deze manier ondertekend is, wordt automatisch gelijkgesteld met een handgetekend document.

Kun je een e-mail aangetekend versturen?

Bij Certipost hebben particulieren de mogelijkheid om e-mails of elektronische documenten aangetekend te verzenden. Maar men onderzoekt ook de uitbreiding daarvan naar de professionele markt. *'Je maakt een account aan met behulp van je elektronische identiteitskaart en verstuurt je e-mail met een eventuele bijlage, zoals je dat normaal doet'*, legt Katrien Buschaert, Head of Marketing bij Certipost, uit. *'Alleen vul je een postadres in en geen e-mailadres. Vervolgens wordt je bericht afgeprint en in een enveloppe gestopt in een beveiligde ruimte. Daarna wordt het aangetekend verzonden met de post. Het gaat hier dus om een hybride vorm, waarbij de afzender heel wat tijd wint en de*



Ywein Van den Brande: *'In rechtszaken wordt steeds vaker rekening gehouden met mailverkeer.'*

Hans Graux:
'Vertrouwelijkheid, wat mag en niet, kan extra benadrukt worden in het contract zelf.'

bestemmeling niet eens merkt dat het om een elektronisch aangetekende zending gaat.'

Maar Hans Graux, advocaat bij time.lex, waarschuwt voor de juridische onduidelijkheid rond elektronisch aangetekende post. *'In mei 2007 is een wet gepubliceerd waarin een aantal elektronische vertrouwensdiensten, zoals archivering,* timestamping *en aangetekend verzenden, algemeen gedefinieerd worden. Maar in die wet staat ook dat er binnen een aantal maanden een Koninklijk Besluit moet volgen met de verdere uitwerking. Hoe moeten deze diensten functioneren? Wat zijn hun verplichtingen? Welke garanties moeten ze bieden? Wat is de juridische waarde? Door de politieke crisis is dat KB er nooit gekomen. Hierdoor kan men dus niet met zekerheid zeggen dat elektronisch aangetekende post gelijkgesteld is aan een aangetekende brief. Een systeem waarbij de aanlevering elektronisch gebeurt, maar het uiteindelijke resultaat wel een aangetekende brief is – zoals bij Certipost –, lijkt me geen probleem.'*

Mag ik als werkgever het elektronisch verkeer van mijn werknemers nakijken?

Dat mag, maar alleen als bepaalde regels – voornamelijk vastgelegd in cao 81 – gerespecteerd worden. Als je als werkgever e-mails, webnavigatie, *instant messaging* of telefonie wilt nakijken, moeten je werknemers daarvan op de hoogte zijn. Bovendien mag je geen maatregelen nemen waarmee je iemand persoonlijk viseert, tenzij daar een gegronde reden voor is. Dat kan bijvoorbeeld een virus op een werkstation zijn, of gedrag dat de economische en financiële belangen van het bedrijf in gedrang brengt. Als het alleen gaat om een mogelijke inbreuk op de regels in het bedrijf – bijvoorbeeld een vermoeden van heel veel persoonlijke mails –, ben je verplicht om de persoon in kwestie eerst te waarschuwen voor je individueel mag controleren.

Bedrijven doen er daarom goed aan om het gebruik van ICT-middelen door personeelsleden duidelijk te omschrijven in een *policy*-document. Wanneer en op welke manier kan er gecontroleerd worden? Wat mag en wat niet? Persoonlijk surfen kan bijvoorbeeld beperkt worden tot de lunchpauze. Wordt het surfgedrag alleen geregistreerd of ook bewaard? Als er een beperking staat op het persoonlijke gebruik van de bedrijfsgsm, vermeld dan meteen ook tot hoeveel minuten of welk bedrag het beperkt is.

Belangrijk is dat een onderneming gebruikmaakt van een zogenaamde 'individuele kennisgeving', waarmee alle werknemers rechtstreeks op de hoogte worden gesteld van de geldende *policy*. Dat kan met een bijlage bij het arbeidscontract, maar ook een mail met updates naar alle medewerkers behoort tot de mogelijkheden. Houd er hoe dan ook rekening mee dat het toezicht op elektronische communicatie zeker geen onbegrensd recht is. Met andere woorden, wie zijn werknemers controleert zonder daarvan iets op papier te hebben staan, riskeert de Wet op de privacy of één van de vele andere wetten te overtreden.

Is mijn bedrijf beschermd door een disclaimer?

Deze e-mail is vertrouwelijk en enkel bedoeld voor de bestemmeling, de inhoud mag niet gekopieerd worden, het bedrijf is niet verantwoordelijk voor eventuele virussen... Een disclaimer onderaan de e-mail bevat heel wat verschillende waarschuwingen, maar vaak zijn die onzinnig.

'De verantwoordelijkheid voor de inhoud van de e-mail afwijzen, is ook contradictorisch', waarschuwt Jos Dumortier, professor ICT-recht aan de K.U.Leuven en advocaat bij time.lex. *'Als je een offerte ontvangt via mail maar je het bedrijf nooit aansprakelijk kunt stellen voor de inhoud van die e-mail, wat betekent dat dan? Men schrijft vaak ook dat men niet verantwoordelijk is voor eventuele virussen, maar dit is eigenlijk een "exoneratieclausule". Met andere woorden, die moet door de andere partij aanvaard worden, wat bij een e-mail duidelijk niet het geval is.'*

Nuttiger is het om boven- of onderaan de e-mail een link te plaatsen naar de beleidsverklaring en de privacy *policy* over het gebruik van communicatiemiddelen.

Moet ik bang zijn voor een aanval?

'Hackers willen zo snel mogelijk geld verdienen', stelt Eddy Willems, Security Evangelist bij Kaspersky en Director Information and Press bij het European Institute for Computer Antivirus Research (EICAR). *'Dat betekent dat HR-gegevens voor hen niet echt interessant zijn. In de praktijk wordt dan ook zelden in dergelijke systemen ingebroken. Bovendien maken hackers gebruik van onvolkomenheden in de toepassing. Ze moeten dus eerst 100 procent op de hoogte zijn van het systeem dat in jouw bedrijf gebruikt wordt. Aangezien de buitenwereld niet kan zien op welk e-HR-platform je werkt, is het gevaar beperkt.'*

Anderzijds waarschuwt Willems wel voor het groeiend aantal varianten en de ernst van malware. *'Vroeger had je vooral virussen, wormen, spam en trojans. Maar nu krijg je ook te maken met keystroke loggers, spyware, adware, phishing, bots... Elke seconde duikt nieuwe malware op. Je kunt dus maar beter over een goed beveiligingspakket beschikken, dat bovendien correct is ingesteld én dagelijks geüpdatet wordt. Een degelijke firewall moet de ongebruikte poorten blokkeren.'*

Hoe veilig zijn paswoorden?

'Gebruik moeilijke paswoorden' is één van de tien tips voor *safe internet security* van de antivirusmaker Kaspersky. De vraag is natuurlijk wat je onder 'moeilijk' moet verstaan? *'Applicaties moet je inderdaad beveiligen met sterke paswoorden en dat is vaak het grootste struikelblok'*, zegt Eddy Willems van Kaspersky. *'Paswoorden zijn vaak veel te voor de hand liggend en te gemakkelijk. Een paar lettertjes in combinatie met een paar cijfertjes is eigenlijk niet voldoende. Het is beter om een volledige zin als paswoord te nemen, bijvoorbeeld "Ik zit op 16 juni op een conferentie in Nederland".'*

Mag ik confidentialiteit verwachten van mijn werknemers?

Confidentialiteit valt in principe onder de plicht in het arbeidsrecht dat elke werknemer zich zorgvuldig moet gedragen bij het uitvoeren van zijn taken. Dat wil zeggen dat hij niet zomaar vertrouwelijke informatie mag vrijgeven of laten rondslingeren, bijvoorbeeld op een gedeelde printer. Als dat toch gebeurt, kijk je best naar de gevolgen van die actie. Jaarcijfers die te vroeg publiek gemaakt worden, is bijvoorbeeld minder gevoelige informatie dan persoonlijke evaluaties of medische gegevens. Iemand die een kleine fout maakt, kan er met een waarschuwing van af komen, een grote fout wordt bestraft met ontslag.

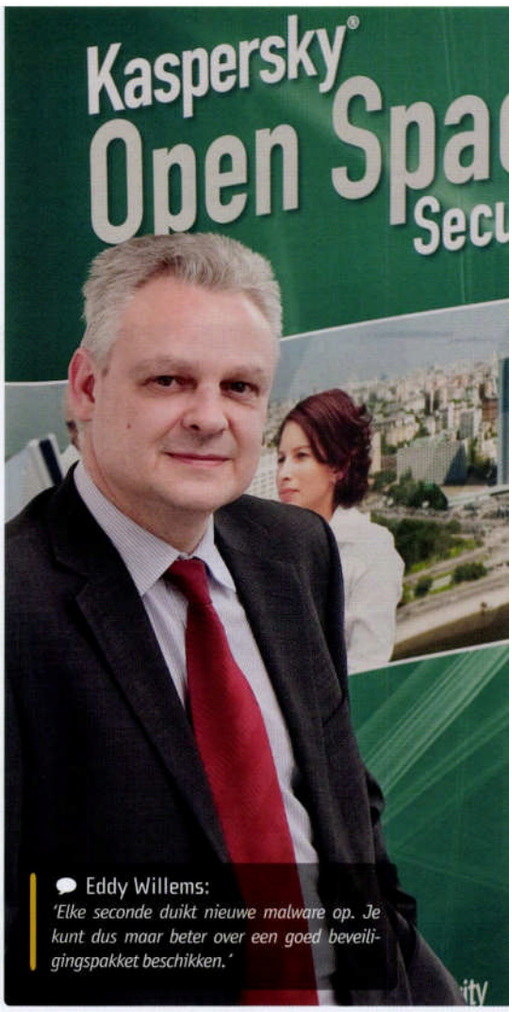
'Een open communicatie en duidelijke richtlijnen zijn natuurlijk het best', zegt advocaat Hans Graux. *'Bij bepaalde functies krijgt men constant vertrouwelijke informatie te verwerken; denk aan een HR-assistant die overal toegang tot heeft. In die gevallen kan de vertrouwelijkheid en wat mag en niet mag nog eens extra benadrukt worden in het contract zelf.'*

Kan ik een werknemer ontslaan voor dingen die hij of zij publiceert op internet?

Eigen websites, blogs, socialenetwerksites... Het lijkt wel alsof iedereen actief is op internet. Toch moet je dat voorzichtig aanpakken. *'Er zijn gevallen bekend waarbij een werknemer werd ontslagen nadat hij op* Facebook *een video plaatste waarin hij zijn werkgever op een grove en onterechte manier bekritiseerde'*, weet Hans Graux. *'Als werknemer ben je verplicht om je loyaal op te stellen ten opzichte van je werkgever, dus voor zoiets kun je wel degelijk ontslagen worden. Als bedrijf moet je dan wel zeker zijn dat je het bewijsmateriaal in handen hebt, anders is achteraf betwisting mogelijk. Je kunt bijvoorbeeld een proces-verbaal laten opstellen door een deurwaarder. Je staat natuurlijk ook sterk in je schoenen als een klant, als neutrale derde partij, hierover een opmerking heeft gemaakt bij jou, de werkgever.'*

Een tweede heikel punt is het aantonen van de link met de werknemer. *'Bij video's komt de persoon zelf in beeld, dan is er geen twijfel mogelijk'*, zegt Graux. *'Als het gaat om een audiofragment of een geschreven boodschap, ligt dat al wat moeilijker. Je zou een klacht kunnen indienen en een onderzoek laten instellen om te achterhalen welke computer gebruikt is, maar dat is heel omslachtig. Wat men in de praktijk vaak doet, is de werknemer confronteren met de website. Als hij bekent, hoeft dat trouwens nog geen verzachtende omstandigheid te zijn. Zijn medewerking spreekt hem niet vrij van zijn acties, hij kan dus nog steeds ontslagen worden.'*

Als de filmpjes of boodschappen louter privé zijn, ligt de zaak anders. *'Er zal dan naar allerlei factoren worden gekeken: welke functie of rol heeft hij of zij, wat is de aard van de boodschap, wat zijn het imago en de waarden van het bedrijf...? Het kan bijvoorbeeld niet dat iemand die in het onderwijs werkt, elk weekend op* Facebook *publiceert dat hij zich lazarus heeft gedronken. Tegen een filmpje van een strippende helpdeskmedewerker kun je als bedrijf dan weer weinig beginnen'*, aldus Graux.



Eddy Willems:
'Elke seconde duikt nieuwe malware op. Je kunt dus maar beter over een goed beveiligingspakket beschikken.'

Wat moet je in het oog houden bij het gebruik van een laptop van het werk?

'Naast de bedrijfsfirewall heeft elk werkstation ook een eigen firewall', legt Eddy Willems uit. *'Omdat het instellen van die individuele firewall dikwijls zorgt voor heel wat pop-upvensters met vragen, zetten werknemers die vaak uit. Op zich is dat geen probleem, zolang men binnen de bedrijfsomgeving blijft. Bij laptops ligt dat dus gevoelig. Medewerkers gebruiken hun notebook op conferenties, in hotels enzovoort. En als op dat moment geen firewall actief is, hebben hackers het wel heel makkelijk om vertrouwelijke gegevens of documenten te kopiëren. Ofwel moet je als werknemer de discipline aan de dag leggen om bij het vertrek uit het bedrijf telkens de persoonlijke firewall aan te zetten, ofwel laat je de technische dienst de firewall zo instellen, dat je er niet veel last van ondervindt en die dus continu kunt laten aanstaan.'*

TOP 10 SAFE INTERNET SECURITY TIPS VOLGENS ANTIVIRUSMAKER KASPERSKY

1. Maak geregeld back-ups.
2. Controleer frequent of er geen nieuwe updates voor je software beschikbaar zijn.
3. Gebruik geüpgrade antivirus- en spywaresoftware, en controleer geregeld op updates.
4. Stel een persoonlijke desktopfirewall in.
5. Kies moeilijke paswoorden, bij voorkeur hele zinnen.
6. Wees heel voorzichtig met onbekende documenten of programma's.
7. Surf doelgericht en volg een zekere logica bij het aanklikken van links.
8. Denk twee keer na voor je persoonlijke gegevens achterlaat.
9. Reageer niet op spam.
10. Gebruik je gezond verstand!