Zwerfinformatie

Zonder omwegen goed en veilig werken met informatie

Benchmark over informatieveiligheid

veenman

Inhoud

Voorwoord 03

Inleiding 04

Hoofdstuk 01 | **Groeiende veiligheidsrisico's** 06

Hoofdstuk 02 | **Veiligheidsbewustzijn en verantwoordelijkheid** 16

Hoofdstuk 03 | **Veiligheidsbeleid en maatregelen** 30

Hoofdstuk 04 | **Conclusies en aanbevelingen** 44

Over Veenman 48

Voorwoord

Het MKB, zowel de kleinere als de grotere organisaties, staat voor de uitdaging te investeren in technologie om informatieveiligheid te waarborgen. Maar als medewerkers niet bewust met de risico's omgaan, helpt zelfs de meest geavanceerde technologie niet. Denk bijvoorbeeld aan het klikken op een schadelijke link in een e-mail of het gebruik van diensten, zoals Dropbox en WeTransfer, om zakelijke informatie uit te wisselen.

Daarnaast slingert bij veel organisaties informatie rond: 'zwerfinformatie' als het ware. Het betreft bijvoorbeeld prints of USB-sticks die achterblijven op de werkplek of een e-mail met een bijlage met salarisgegevens die per ongeluk aan de verkeerde personen wordt gestuurd. Maar denk ook aan werknemers die hun laptop in de auto laten liggen. Als die laptop vervolgens gestolen wordt, ligt alle bedrijfsinformatie op straat. Als het dan ook nog privacygevoelige informatie betreft, moet dat zelfs officieel gemeld worden bij de Autoriteit Persoonsgegevens.

De manier waarop mensen met informatie omgaan kan dus risico's opleveren. Hoe bewust zijn medewerkers zich daarvan? En wat doen organisaties om het bewustzijn te vergroten? Ligt de focus op de techniek of de gedragskant, of zijn beide belangrijk? We hebben daarom deze en andere vragen voorgelegd aan uw collega's in verschillende branches. In dit rapport presenteren we hun antwoorden.

Opmerkelijk is dat veel ondervraagden denken dat het gevaar van buiten komt, terwijl de dreiging van binnenuit juist veel groter is. Daarnaast voelt slechts een op de vijf werknemers zich verantwoordelijk voor de veiligheid! De respondenten onderschrijven dat zwerfinformatie het grootste veiligheidsrisico vormt. Hier stuiten we op 'witte vlekken'.

Het is dus de hoogste tijd om deze witte vlekken weg te werken! Hoe kan zwerfinformatie het beste worden tegengegaan en hoe kan het gedrag van medewerkers effectief worden verbeterd? Oftewel: hoe kunnen we het symptoom zwerfinformatie bestrijden?

De expertise van Veenman ligt in het slim omgaan met informatie en informatiebeveiliging. Wij kunnen u de nodige adviezen geven en samen met u de zwerfinformatie in uw organisatie aanpakken.

P.S. Onze dank gaat uit naar alle deelnemers aan het onderzoek!
Januari 2017

Wilco van Bezooijen
Algemeen Directeur
Veenman

Inleiding

Dit rapport bevat de belangrijkste bevindingen uit de benchmark over de veiligheidssituatie bij informatie-intensieve organisaties.

De onderzoeksperiode liep van augustus tot november 2016. Het onderzoek is uitgevoerd op initiatief van Veenman door ProSpex BV. Veenman is specialist in geïntegreerde oplossingen voor informatiemanagement. In totaal hebben bijna 170 personen deelgenomen aan het onderzoek. Uit de hoge respons is af te leiden dat het onderwerp sterk leeft onder de doelgroep.

Sectoren waarin de deelnemers actief zijn

De hoogste respons kwam van zakelijke dienstverleners (26%). Ook financiële dienstverleners (13%) en overheden (17%) zijn ruim vertegenwoordigd. In deze sectoren worden zaken rond informatieveiligheid steeds strenger gereguleerd. Verder is bijna een kwart van de respondenten actief in de zorg. Daar is sprake van een exploderende hoeveelheid informatie en de invoering van het veelbesproken elektronisch patiëntendossier. Er hebben ook ICT-bedrijven deelgenomen. Deze hebben veel te maken met informatiebeveiliging (voor klanten).

Functie van de deelnemers

We zien dat het onderwerp informatieveiligheid brede interesse heeft binnen organisaties. Het zwaartepunt van de deelnemers ligt bij ICT-managers (25%). Information security officers en leden van de algemene directie zijn beide goed voor 16% van de respons. Daarnaast is de financiële directie met 5% vertegenwoordigd.

Aantal medewerkers en vestigingen

De grootte van de organisaties is van invloed op de wijze waarop men omgaat met informatieveiligheid. In dit onderzoek heeft 33% van de organisaties tussen de 20 en 100 medewerkers, 19% tussen de 100 en 1.000 medewerkers en 17% meer dan 1.000. Ook de fysieke structuur van een organisatie is van invloed op de informatieveiligheid. Wanneer de werkzaamheden op meerdere locaties worden uitgevoerd, stijgen de veiligheidsrisico's. Ruim de helft van de responderende bedrijven heeft 1 tot 10 vestigingen; 40% heeft 11 tot 20 vestigingen. De overige 10% heeft tussen de 20 en 300 vestigingen of meer.

De opbouw van dit rapport

In het eerste hoofdstuk gaan we na wat de belangrijkste risico's zijn op het gebied van informatieveiligheid en waardoor deze risico's worden veroorzaakt. Het tweede hoofdstuk belicht het veiligheidsbewustzijn van medewerkers en de verantwoordelijkheid hiervoor. In het derde hoofdstuk komen het beleid en de maatregelen aan bod die organisaties genomen hebben om de informatieveiligheid te waarborgen. In het laatste hoofdstuk staan de conclusies en aanbevelingen.

In welke sectoren zijn de respondenten actief?

Antwoord	
Zakelijke dienstverlening	**26%**
Zorg	**23%**
Overheid	**17%**
Financiële dienstverlening	**13%**
ICT en automatisering	**6%**
Industrie en productie	**3%**
Cultuur & onderwijs	**2%**
Hospitality, recreatie & toerisme	**2%**
Retail en handel	**1%**
Bouw & industrie	**1%**
Energie	**1%**
Transport en logistiek	**1%**
Anders	**4%**

Wat is de functie van de deelnemende respondenten?

Antwoord	
ICT-manager	**25%**
Informatie Security Manager	**16%**
Directie Algemeen	**16%**
Directie Financieel	**5%**
HR-manager	**4%**
Controller	**4%**
Afdelingsmanager	**4%**
Sales & Advies	**4%**
Anders	**22%**

Hoofdstuk 01

Groeiende veiligheidsrisico's

Fysiek rondzwervende informatie is het grootste risico

Gevoelige informatie die in de prullenbak wordt gegooid of voor iedereen zichtbaar op bureaus ligt en niet-opgehaalde prints worden door alle respondenten genoemd als grootste risico voor de informatieveiligheid. Op twee staat het gebruik van USB-sticks die vaak voor het grijpen liggen of in een (flex) computer blijven zitten (75%). Hackers staan pas op de derde plaats in de risicolijst (73%). Eigen onachtzaamheid wordt dus als een groter probleem gezien dan digitale inbraak. Eigen smartphones en tablets die voor het werk gebruikt worden zijn voor 68% van de respondenten een punt van zorg. Verder noemt 66% het uitwisselen van bestanden via publieke sites als WeTransfer, iCloud en Google Drive een risicofactor.

Ontslagen medewerkers die nog toegang tot bedrijfsinformatie hebben, worden door 40% van de deelnemers genoemd als veiligheidsrisico. Over de gevaren van werken via openbare wifispots of het lekken van data via sociale media maakt maar een kwart zich zorgen, terwijl mensen zich juist daar impulsief manifesteren. Ook apps die toegang geven tot contactlijsten van privé smartphones worden slechts door een minderheid van 21% als risico gezien.

In de categorie Anders noemt men het fenomeen social engineering. Hierbij wordt alle informatie van personen die online beschikbaar is, samengevoegd tot een profiel op basis waarvan hackers acties uitzetten. Die acties worden door medewerkers vertrouwd,

Welke van de onderstaande zaken vormen volgens u de grootste risico's voor de informatieveiligheid in uw organisatie?

Antwoord	
Rondslingerend papier (niet opgehaalde prints op printers, files op bureaus, papier in prullenmanden,...)	**100%**
USB-sticks	**75%**
Hackers	**73%**
Privé smartphones en tablets die voor het werk gebruikt worden	**68%**
Bestandsuitwisseling via openbare sites als WeTransfer, iCloud en Google Drive	**66%**
Memostickers met wachtwoorden	**41%**
Ontslagen medewerkers die nog over informatie beschikken	**40%**
Openbare wifispots	**27%**
Sociale media	**23%**
Apps die toegang vragen tot contactlijsten	**21%**
Bluetoothverbindingen	**5%**

omdat ze vanuit hun sociale kring lijken te komen door de ‘intieme’ informatie die berichten bevatten. Ook onwetendheid van gebruikers wordt genoemd in de categorie Anders. Kennelijk zijn niet alle medewerkers alert op malware en ander onheil dat digitaal kan binnenkomen door klakkeloos e-mails te openen.

Conclusie: het informatieveiligheidsbewustzijn van medewerkers dient brede aandacht te krijgen, omdat de risico’s niet alleen in de computers zitten, maar vooral te maken hebben met menselijk handelen. Hierna gaan we nader in op trends die de genoemde veiligheidsrisico’s vergroten.

Uitbreiding van het aantal communicatiekanalen

Telefoon en e-mail zijn nog steeds de meest gebruikte communicatiemiddelen. Printen is al niet meer voor iedereen vanzelfsprekend. Nog maar 80% van de respondenten meldt via prints te communiceren. Opvallender is dat 50% van de deelnemende organisaties aangeeft ook via sociale media, videoconferencing en chats te communiceren. Het is de vraag hoe veilig dit gebeurt. Wanneer informatie in onbevoegde handen valt, omdat deze via (semi-)openbare netwerken wordt uitgewisseld, is de (reputatie)schade veelal niet te overzien.

Via welke kanalen en instrumenten wisselen uw medewerkers informatie uit met elkaar en met uw klanten? (meerdere antwoorden mogelijk)

Antwoord	
Telefoon	**100%**
E-mail	**100%**
Print	**80%**
Intra- of extranet	**65%**
Sociale media	**40%**
Sms	**36%**
Videoconferencing	**25%**
Chat	**24%**
Anders	**15%**

Sociale media worden ook zakelijk ingezet

In de ‘connected world’ heeft iedereen te maken met informatieveiligheid. Het raakt ons allemaal, zowel zakelijk als privé. Maar hoe zijn we ermee bezig? Zijn we bewust onbekwaam, weten we het ergens wel, maar denken we dat het zo’n vaart niet zal lopen? Of zijn we al onbewust bekwaam? Hebben we een zesde zintuig ontwikkeld om verkeerde handelingen te vermijden? Het antwoord begint met de vraag welke media medewerkers gebruiken voor het uitwisselen van informatie.

Welke social media gebruikt u voor het uitwisselen van zakelijke informatie?

Antwoord	
Facebook	**38%**
Twitter	**27%**
Linkedin	**19%**
WhatsApp	**11%**
Instagram	**1%**
YouTube	**1%**
Bloggen	**1%**
Yammer	**1%**
Zoho Connect	**1%**

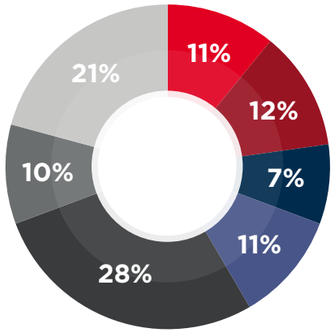
We zien dat tools die groot zijn geworden in een consumentenomgeving nu ook het kantoor veroveren. Facebook wordt door 38% van de deelnemers gebruikt en Twitter door 27%. Doorvragen leert dat sommige bedrijven een beleid voor sociale media hebben ontwikkeld. Dat beleid kan een verbod op het gebruik van sociale media inhouden of het bestaat uit richtlijnen. Verder gebruikt 19% LinkedIn, dat uitgroeit van een cv-bank naar een platform waarop professionals informatie uitwisselen. **Eigenlijk zien we op alle platforms een verschuiving van raadplegen en zenden naar verbinden en delen.** In dit kader wordt ook een samenwerkingsplatform als Yammer genoemd. Hoe gaan we om met al die vormen van sociale media? Nu Facebook en LinkedIn steeds vaker de digitale sleutel tot andere portalen worden, is het zaak de kruisbestuiving van informatie goed in de gaten te houden.

Groeiend gebruik van schaduw-IT

Tien jaar geleden verliep de communicatie tussen medewerkers en met klanten vrijwel volledig via beveiligde bedrijfssystemen. Sindsdien is het aantal media voor het uitwisselen van informatie razendsnel gegroeid. Medewerkers willen in hun werksituatie net zo makkelijk kunnen communiceren als in hun privésituatie. Vandaar dat toepassingen voor particulier gebruik, die kosteloos via het openbare internet beschikbaar zijn, ook steeds vaker worden gebruikt in zakelijke omgevingen. Door deze ontwikkeling verliest de organisatie het zicht en de controle op de veiligheid en integriteit van de informatiestromen. Dat schaduw-IT een belangrijk

punt is, blijkt uit het feit dat opgeteld 41% van de organisaties aangeeft dat minimaal de helft van de medewerkers gebruik maakt van tools als Skype, Snapchat, WhatsApp, Dropbox en WeTransfer voor bedrijfscommunicatie.

Hoeveel procent van de medewerkers binnen uw organisatie gebruikt gratis tools zoals Skype, Snapchat, WhatsApp, Dropbox, WeTransfer, etc. om binnen uw organisatie samen te werken, te communiceren en informatie te delen?



Antwoord
- 75% - 100%
- 50% - 75%
- 25% - 50%
- 10% - 25%
- 1 - 10%
- Geen
- Geen idee

Publieke chat apps voor zakelijke doelen

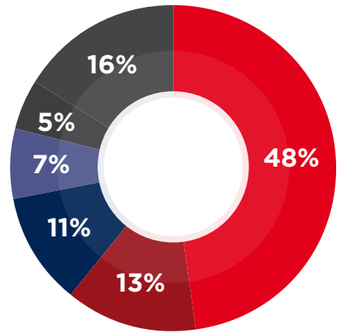
De mix van communicatiemiddelen blijft veranderen. Naar verwachting zal sms onder meer terrein verliezen aan chat apps. Sommige organisaties hebben een eigen en beveiligde omgeving ingericht voor videochatting, met name middels Skype for business. Maar het gros van de respondenten gebruikt WhatsApp (48%). Daardoor wordt de grens tussen privé en zakelijk flinterdun. Sommige respondenten melden wel dat het gebruik van WhatsApp zeer beperkt is en dat er regels zijn opgesteld over wat wel en niet uitgewisseld mag worden. Ook Facebook Messenger staat in de top 3 van zakelijke chatomgevingen. Conclusie is dat voor een groot deel van de communicatie schaduw IT-applicaties gebruikt worden, met alle risico's van dien.

De opmars van multifunctionele oplossingen

Naast de standaard tekstberichten en emoticons kunnen steeds meer andere vormen van digitale informatie via chats gedeeld worden. Ook chattools bieden nieuwe mogelijkheden voor online samenwerken. Maar gebruikers willen eigenlijk een one-stop-tool voor al hun communicatiebehoeften. Dus geen aparte programma's voor chatten, videoconferencing, het delen van documenten, agendabeheer en het vinden van (interne) experts. Daarom veroveren tools met een scala aan dedicated oplossingen de zakelijke markt. Namen die de respondenten in dit verband noemen zijn onder meer Jabber, Slack en Google+.

Consumenten-tools dreigen de zakelijke communicatie over te nemen

Via welke chat-applicatie(s) wordt informatie uitgewisseld?

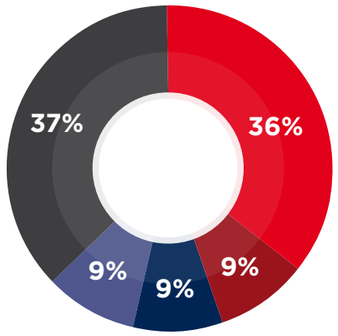


Antwoord
- WhatsApp
- Professionele bedrijfsapplicaties (MS Lync, Jabber, SalesForce, WeChat)
- MS Skype for business
- Facebook Messenger
- Sms
- Anders

Publiekstool voor videoconferencing

De oplossingen die we voor chatting tegenkomen zien we deels ook bij videoconferencing terug, hoewel de percentages anders liggen. De meeste respondenten (37%) gebruiken Skype, dat is overgenomen door Microsoft. Het gaat hier om de gratis publieke versie. Microsoft biedt inmiddels ook Skype for business, maar dit wordt door slechts 11% gebruikt. Lync (ook Microsoft) en Lifesize worden vaker genoemd als middel voor videoconferencing en chats op het werk.

Welke toepassingen voor videoconferencing gebruikt uw organisatie?



Antwoord

- Skype
- Onbekend
- Lifesize
- Lync
- Anders

Bestanden zwerven rond over verschillende media

De informatie die we creëren heeft pas waarde als zoveel mogelijk mensen er iets mee doen. Als informatie gaat reizen, proberen organisaties daar grip op te krijgen. **Maar bestanden zijn net water: ze zoeken altijd de weg van de minste weerstand.** In veel organisaties leidt het beperken van de bestandsgrootte op de mailservers tot het zoeken naar alternatieven. Sommige bedrijven schaffen het gebruik van e-mail zelfs helemaal af om ‘information overload’ te voorkomen. Daardoor groeit het gebruik van WeTransfer (74%) en Dropbox (27%). Verder gebruiken werknemers hun privéaccount voor Google Gmail om grote bestanden te versturen. Om in control te blijven biedt 29% van de organisaties werknemers een FTP-server als alternatief.

E-mail is nu nog het meest gebruikte middel voor gegevensuitwisseling (100%). Maar er worden meestal limieten gesteld aan de omvang van bijlagen. Systeembeheerders willen tenslotte de e-mailservers niet laten volstromen. Om die reden heeft 99% van de organisaties een netwerkschijf waar bestanden opgeslagen en gedeeld kunnen worden. Maar deze centrale dataopslag is vaak niet overal en niet voor iedereen toegankelijk.

De USB-stick is bij 41% van de organisaties in gebruik als middel voor het uitwisselen van bestanden en documenten. Het formaat blijft klein, maar de sticks kunnen steeds grotere hoeveelheden data bevatten. Daarnaast bedient men zich van platforms waarop de structuur voor het vastleggen en delen van bestanden al vooraf is bepaald. Denk hierbij aan SharePoint (27%). Het aanbod aan oplossingen voor bestandsuitwisseling is groot.

Van de ondervraagden gebruikt 21% specifieke oplossingen als Cryptshare, eigen portalen, Filecap, 7Zip, Document Management Systeem, Gemnet en Acronis Access. Ook wordt specifieke software ingezet voor bestandsuitwisseling door gemeenten en zorginstellingen.

Hoe delen medewerkers grote bestanden met collega’s, klanten of leveranciers?

Antwoord	
Zakelijke e-mail	**100%**
Netwerkschijf	**99%**
WeTransfer	**74%**
USB-stick	**41%**
FTP-server	**29%**
SharePoint	**27%**
Dropbox	**27%**
Via andere online fileshare applicaties als: FileBox, SyncFile, 7Zip DMS, DocuShare. Filecap, Cryptshare, Google Drive	**21%**
Eigen portal, eigen cloud	**11%**
Privé e-mail	**6%**
Brancheportaal, elektronisch dossier, zorgmail	**4%**
Niet	**1%**
Op papier	**1%**


Bestanden zijn net water:
ze zoeken altijd de weg van
de minste weerstand.
veenman

Hoofdstuk 02

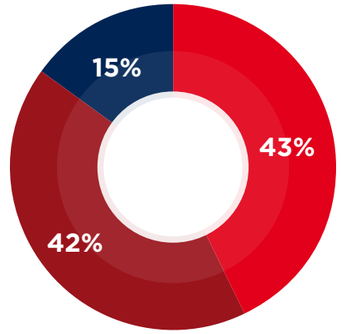
Veiligheidsbewustzijn en verantwoordelijkheid

Risico's van openbare netwerken vaak niet bekend

Door het gemak waarmee mensen communicatietools kunnen gebruiken, verdiepen ze zich er niet echt in. Dat is een risico. De informatie die we delen op platforms voor sociale media mag meestal niet door iedereen gezien worden. Maar wie is op de hoogte van alle instellingen van die platforms? Waar staat de informatie eigenlijk? En is het veilig als je via een openbaar netwerk het internet op gaat of kijken er dan mensen mee?

Het risicobewustzijn begint te komen, maar we zijn er nog lang niet. Minder dan de helft (42%) scoort een voldoende als gevraagd wordt hoe bekend medewerkers zijn met de veiligheidsrisico's van openbare netwerken. Van de rest is 15% volledig onbekend met de risico's en 42% kan hier geen uitspraak over doen. Ook dat is zorgelijk. Als niet duidelijk is door welke handelingen risico's ontstaan, gaan medewerkers ongewild de fout in.

In hoeverre zijn medewerkers bekend met de risico's die het gebruik van computers en mobile devices op openbare netwerken meebrengen?



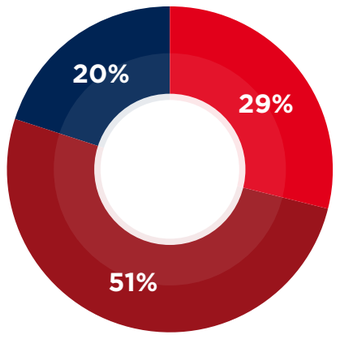
Antwoord

- (volledig) bekend
- neutraal
- (volledig) onbekend

Onduidelijkheid over de risico's van zwerfinformatie

Iedere vorm van informatieoverdracht heeft eigen karakteristieken en derhalve eigen risico's. Het is duidelijk dat het laten rondslingeren van prints en scans risicovol is. Met messaging en videocalling wordt het al een stuk schimmiger. Welke weg legt informatie af voordat deze bij de ontvanger aankomt? Bijna 30% is zich (volledig) bewust van de risico's die kunnen ontstaan door de manier waarop men omgaat met printen, scannen, messaging en videocalls. Bij deze organisaties weten medewerkers welk informatiespoor ze achterlaten. Ruim de helft van de respondenten is daar niet zo zeker van. Deze denken dat medewerkers de risico's niet kennen of zich daar niet van bewust zijn in hun handelingen. Kun je ze dat verwijten als hun organisatie geen goede voorlichting biedt en geen procedures heeft?

In hoeverre zijn uw medewerkers zich bewust van de risico's die ontstaan door de wijze waarop ze omgaan met printen, scannen, messaging, videocalls en de gerelateerde informatiesporen?



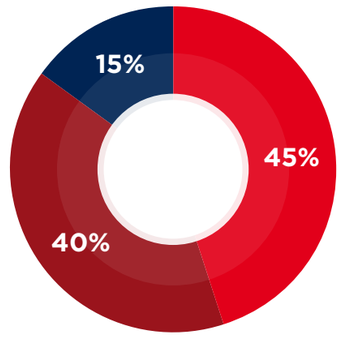
Weinig eigen verantwoordelijkheid voor veilig werken

Volgens 70% van de responderende organisaties zijn werknemers niet zelf verantwoordelijk voor informatieveilig werken. Ze leven in de veronderstelling dat dit met beveiligde IT-voorzieningen en beleid is te waarborgen. Maar eerder is al aangetoond dat medewerkers steeds meer publieke tools en netwerken gebruiken om informatie uit te wisselen en dat ze hiervoor vaker eigen apparatuur gebruiken. Het toenemend gebruik van schaduw-IT en de opkomst van Bring-Your-Own-Device vraagt meer veiligheidsbewustzijn van medewerkers. Wanneer dit ontbreekt, kunnen zij hackers ongewild een entree verschaffen met alle kwalijke gevolgen van dien.

Bewustzijn van privacygevoelige informatie

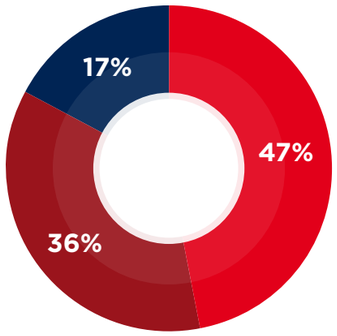
Privacy is een groot goed, maar privacybewustzijn is iets waar we onszelf eigenlijk pas relatief kort van bewust worden. Wat betekent privacy eigenlijk en wanneer wordt er inbreuk gemaakt op iemands privacy? Wanneer betreden we de beschermde zone rond een individu, of dat nu een medewerker, een klant, een patiënt of een anonieme bezoeker van onze website is? Zijn medewerkers zich bewust van de risico's die het werken met privacygevoelige informatie meebrengt? Bij 45% van de bedrijven weten medewerkers wat de mogelijke directe en indirecte schade kan zijn. Daartegenover staat een groep van 40% die hier geen duidelijke uitspraak over durft te doen. En 15% meldt zelfs dat medewerkers te weinig kennis hebben over de gevolgen die het lekken van privacygevoelige informatie kan hebben.

In hoeverre zijn uw medewerkers zich bewust van de directe en indirecte schade die kan ontstaan door onachtzaam gedrag met betrekking tot privacygevoelige informatie?



Bewustzijn van concurrentiegevoelige informatie
R&D resultaten, voorraadcijfers, klantenlijsten, ordervolumes, marketingplannen, personeelsbestanden, alle bedrijfsinformatie heeft waarde voor de concurrentie. Zeker in markten waar bedrijven miljoenen investeren in product- en marktontwikkeling. Bedrijfsspionage is dan ook zeer lucratief. Toch zijn medewerkers bij ruim de helft van de respondenten zich er niet van bewust dat ze met concurrentiegevoelige informatie werken. Zij staan er niet bij stil (36%) of beseffen niet dat de informatie waarmee ze werken of waartoe ze toegang hebben voor anderen van waarde kan zijn (17%).

In hoeverre zijn medewerkers zich bewust van de waarde van de informatie en het informatienetwerk waar ze mee werken? Denk aan concurrentiegevoelige informatie.



Antwoord
(volledig) bewust
neutraal
(volledig) onbewust

Column

Privacy is niet alleen ICT-beveiliging
Organisaties moeten nu echt aan de slag om te zorgen dat ze in 2018 aan de nieuwe privacyregels voldoen. Bedrijven met een grootschalige verwerking van persoonsgegevens moeten bijvoorbeeld een privacyadministratie bijhouden en de verantwoordelijkheid voor het beheer van die gegevens neerleggen bij een functionaris gegevensbescherming (FG) of in het Engels: data protection officer (DPO).

In mei 2018 vervangt de nieuwe Europese privacyverordening de Nederlandse Wet bescherming persoonsgegevens. De grootste verandering van de Europese privacyverordening (officiële naam: General Data Protection Regulation, GDPR) voor het bedrijfsleven is de zwaardere documentatieplicht. Welke data worden er verzameld? Via welke bronnen? Met welke systemen? Hoe zijn die systemen beveiligd? Wie kunnen erbij?

Ook worden deze bedrijven in bepaalde gevallen verplicht een speciale functionaris gegevensbescherming (FG) oftewel data protection officer (DPO) aan te stellen. Deze ziet toe op de omgang met (persoons) gegevens en controleert of de organisatie voldoet aan de wet- en regelgeving.

In de benchmark wordt door geen van de respondenten de FG genoemd. Die functie was al in de Wbp opgenomen en ook in de GDPR staat een uitgebreide beschrijving van de positie, taken en verantwoordelijkheden van de FG. Dit geeft aan dat het gaat om een bijzondere en unieke functie. Gezien de brede deskundigheid die nodig is, gaat het eigenlijk om een schaap met vijf poten. Deze functie doe je er ook niet zomaar ‘even’ bij.

Privacy is niet alleen ICT-security, daar komt echt veel meer bij kijken. Privacy is een zaak van de gehele onderneming, van hoog tot laag. De FG is de spin in het web om iedereen in de organisatie, van hoog tot laag, bewust te maken, te trainen, te auditen. Daarbij wordt hij ondersteund door de diverse functies in de organisatie die daar ook een verantwoordelijkheid in hebben. Dan komt het met het informatieveilig werken en de privacygevoelige zwerfinformatie ook wel goed.

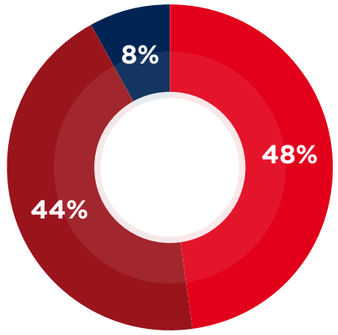
Olga Javornik
ICT-consultant en privacy officer in de juridische praktijk

Invloed van de media op veiligheids-bewustzijn

Overheden en banken voeren regelmatig campagnes om consumenten te waarschuwen tegen cybercriminaliteit, bijvoorbeeld phishing. Hebben die campagnes ook effect op het veiligheidsbewustzijn in de werksituatie? Is het verantwoordelijkheidsgevoel van medewerkers groot genoeg? En speelt het een rol dat ze geen eigenaar zijn van het bedrijf waar ze werken, waardoor ze misschien niet zelf direct geraakt worden als hun organisatie het slachtoffer wordt van cybercrime? Berichten over de grootste bankroof ter wereld, waarin hackers meer dan 100 miljoen dollar hebben buitgemaakt, zijn al snel weer vergeten. Maar als een familielid al zijn spaargeld kwijt is omdat hij zijn bankgegevens rechtstreeks heeft ingevoerd in een hackerssite, dan komt het erg dichtbij en zullen mensen dat onthouden.

Het is dus zaak om de effecten van de cybercrime ook in zakelijke omgevingen zichtbaar te maken. Dat is een permanent proces, want bedrijven en werknemers adopteren in hoog tempo nieuwe technologieën. Zijn meldingen over cybercrime in de media van invloed op het gedrag van de medewerkers? Bij 44% van de respondenten is dat niet het geval. Daar stellen medewerkers geen vragen over de informatieveiligheid naar aanleiding van meldingen. Nog eens 8% geeft aan hier geen zicht op te hebben. Doorvragen bij de rest van de respondenten leert dat medewerkers het onder elkaar wel over berichten in de media hebben. Verder krijgen ze soms berichten doorgespeeld van de ICT-afdeling.

Hebben meldingen over cybercrime in de media impact op het gedrag van de medewerkers?

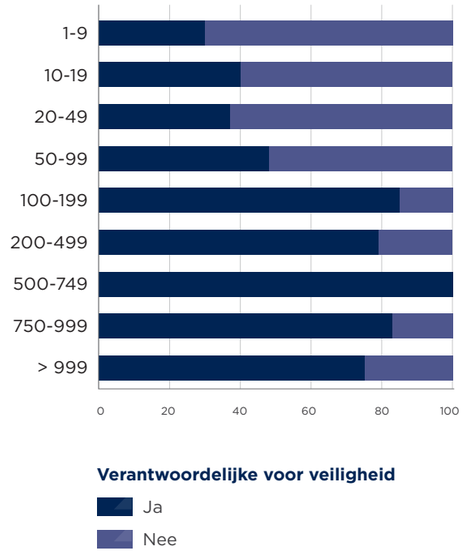


De bedrijfsomvang bepaalt het aanstellen van een formeel verantwoordelijke

Op de vraag of iemand binnen de organisatie formeel verantwoordelijk is voor informatieveiligheid antwoordt 62% bevestigend. Omgekeerd is er bij 38% geen duidelijke contactpersoon die verantwoordelijk is voor grip op de veiligheidssituatie. Daarmee is er geen centraal contact bij een calamiteit. Waar hangt het aanstellen van een verantwoordelijke vanaf?

We hebben gekeken of het aanstellen van een formeel verantwoordelijke voor informatieveiligheid gerelateerd is aan de omvang van de organisatie. Daarbij zien we een opgaande lijn tot de grootte van 500-750 medewerkers. Daarboven zal deze verantwoordelijkheid binnen verschillende functies gedeeld worden of raakt de persoon mogelijk buiten beeld door de omvang van de organisatie.

Organisatiegrootte in relatie tot de aanstelling van een formeel verantwoordelijke voor informatieveiligheid



Breed scala aan verantwoordelijken voor informatieveiligheid

Bij ruim een kwart van de organisaties is de ICT-manager nog eindverantwoordelijk voor de informatieveiligheid. De uitvoerende en controlerende macht ligt hier dus bij dezelfde persoon. Dat is geen goede zaak, want ‘de slager keurt zijn eigen vlees’ als er geen toezicht door anderen is. Daarom heeft ook circa een kwart inmiddels een separate manager informatieveiligheid aangesteld. Bij 19% van de organisaties stijgt informatieveiligheid zelfs boven de techniek uit. Daar is een informatiemanager of CIO verantwoordelijk. Dat informatieveiligheid niet overal in een specifieke functie belegd is, blijkt uit het feit dat de directie of het management bij 12% de verantwoordelijkheid heeft. In de branches Overheid en Onderwijs noemt men in dit verband het gemeente-bestuur of het college van bestuur. Verder meldt 6% dat informatieveiligheid de verant-woordelijkheid is van alle medewerkers en geeft 3% aan dat de verantwoordelijkheid een gedeelde functie is van meerdere mensen binnen de organisatie. Controllers en compliancy-medewerkers krijgen bij 3% de verantwoordelijkheid voor informatie-veiligheid toegeschoven.

Wie is binnen uw organisatie formeel verantwoordelijk voor informatie-veiligheid?

Antwoord	
Separate manager informatieveiligheid	**27%**
ICT-manager	**26%**
Informatiemanager / CIO	**19%**
Directie & management	**12%**
Alle medewerkers	**6%**
Gemeentebestuur & college & wethouders	**4%**
Gedeelde / samengestelde verantwoordelijkheid	**3%**
Controller / compliancy	**3%**

Kan de techniek informatieveiligheid volledig garanderen?

Volgens 89% van de respondenten is dat niet het geval. De techniek kan nog zo goed zijn, op het moment dat mensen met computers werken ontstaan zwakke plekken. Naast de juiste beveiligingstechniek speelt ook het organiseren en stimuleren van veilig gedrag een essentiële rol. Respondenten die menen dat informatieveiligheid volledig gegaran-deerd kan worden vanuit de beste technische beveiligingsoplossingen blijken allemaal eindverantwoordelijk te zijn vanuit een ICT-functie.

Directie, management en specialisten nemen het initiatief

De transitie naar informatiebewust werken moet volgens de respondenten op het hoogste niveau aangestuurd worden. De directie en het management worden daarom bovenaan de lijst gezet, op een gedeelde eerste plaats met de interne veiligheidsspecialist. Het is de vraag of deze ook de mens-kant van de bewustwording kan managen. Op de derde plaats vinden we specialistische afdelingen en commissies. Informatieveiligheid lijkt niet langer een standaardtaak van ICT. De vraag is echter of bedrijven ook organisatorisch en bedrijfscultureel klaar zijn voor de verande-ringen die we massaal met elkaar omarmen. Door wie wordt het informatieveiligheids-bewustzijn geïnitieerd en onderhouden? Waar bevinden organisaties zich in de sequentie onbewust onbekwaam - bewust onbekwaam - bewust bekwaam – onbewust bekwaam?

Wie moet ervoor zorgen dat medewer-kers onbewust bekwaam worden in het werken met informatie en het borgen van de informatieveiligheid?

Antwoord	
Directie & management	**26%**
Interne veiligheidsspecialist	**26%**
Afdeling/speciale commissie informatieveiligheid	**16%**
Gedeelde verantwoordelijkheid	**14%**
Extern bureau	**4%**
Afdelingshoofd	**4%**
ICT	**4%**
Directie en bestuur	**2%**
Niet geregeld	**2%**
Interne overlegstructuur	**2%**

Het besef dringt nog onvoldoende door dat informatieveiligheid een gemeenschappelijke verantwoordelijkheid is van alle medewerkers

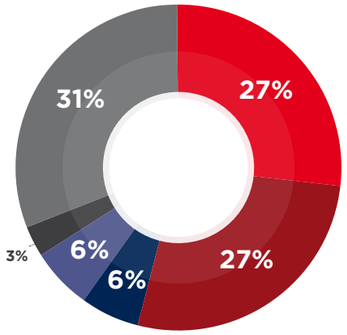
Ook externe assistentie bij bewustzijns-verandering

Informatieveiligheid kent vele betrokkenen en vraagt nieuwe vormen van organiseren. Terwijl afdelingen elkaar moeten vinden in het dynamische informatieveiligheidsdomein doen nieuwe functies en werkgroepen hun intrede. Niet iedereen is even blij met de nieuwe veiligheidstaken en er heerst onduidelijkheid. Op de vraag “Wie moet zorgen dat medewerkers bewust bekwaam worden in het werken met informatie en het borgen van de informatieveiligheid?“ antwoordde één van de deelnemers met “Ikzelf, vrees ik”. En een ander zegt zelfs “Daar zijn we eigenlijk niet of nauwelijks mee bezig.” Daarnaast blijken organisaties op dit nieuwe aandachtsgebied regelmatig externe partijen in te schakelen.

Ligt de primaire verantwoordelijkheid bij de directie of de medewerkers?

Informatieveiligheid kan op allerlei manieren in het geding komen. Wie heeft dan de primaire verantwoordelijkheid volgens de respondenten? De directie is in de ogen van 57% eindverantwoordelijk en bij 9% het lijnmanagement. Slechts 21% vindt dat de medewerkers zelf verantwoordelijk zijn. Alleen deze organisaties beseffen dus dat de gevaren niet zozeer van buiten komen, maar vooral veroorzaakt worden door onachtzaamheid van medewerkers. Die moeten zich bewust zijn van de risico’s en daar naar handelen. De directie en het lijnmanagement kunnen veilig gedrag niet afdwingen omdat het een mentaliteitskwestie is. De vraag is dan ook hoe organisaties het bewustzijn en gedrag van medewerkers kunnen beïnvloeden en hoeveel werk ze daarvan maken.

Wordt het verhogen van het interne veiligheidsbewustzijn door interne of externe partijen opgepakt?



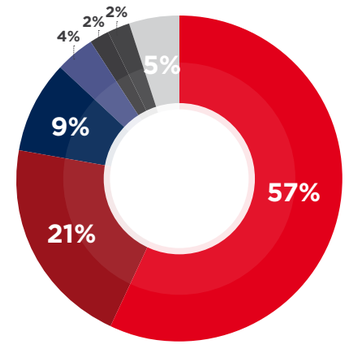
Antwoord

- Dit verzorgt ICT intern
- Dit wordt deels intern en deels door externen verzorgd
- Dit verzorgt HR
- Dit verzorgt de trainingsafdeling
- Dit wordt door een extern bureau verzorgd
- Anders

Op weg naar gemeenschappelijke verantwoordelijkheid

De formele verantwoordelijkheid voor informatieveiligheid heeft geen standaardplek in organisaties. Een groeiend aantal specialisten vervult de functie, die vaak gerelateerd is aan de technologie. Maar het besef dat informatieveiligheid een gemeenschappelijk belang en dus een gemeenschappelijke verantwoordelijkheid is, neemt toe. Je kunt iemand speciaal aanstellen voor de informatieveiligheid, maar daarmee is de veiligheid absoluut nog niet gewaarborgd. Het vormt een vertrekpunt. Waar leggen de aangewezen verantwoordelijken vervolgens het accent in de aanpak vanuit hun functie? Zoeken ze oplossingen voornamelijk in de techniek? Sturen ze op gedrag? Richten ze zich op het versterken van een collectief verantwoordelijkheidsgevoel?

Waar ligt de primaire verantwoordelijkheid voor informatieveiligheid?



Antwoord

- Directie
- Medewerkers
- Management
- Informatiemanager
- ICT-afdeling
- Security manager
- Anders

Hoofdstuk 03

Veiligheidsbeleid en maatregelen

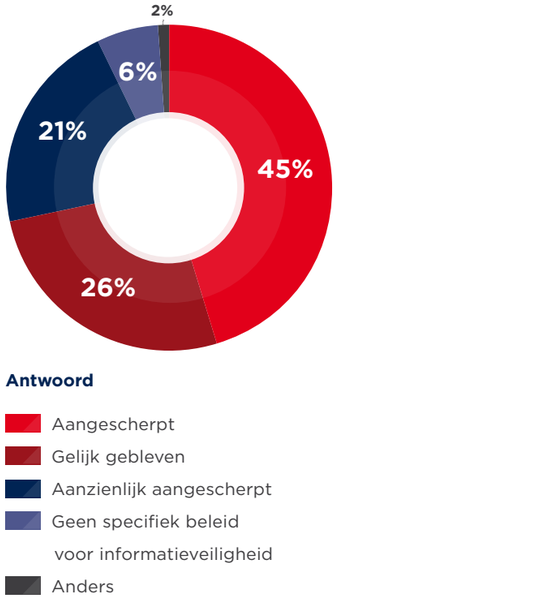
Driekwart van de organisaties heeft het beleid aangescherpt
In totaal heeft 45% van de respondenten het veiligheidsbeleid in de afgelopen 12 maanden aangescherpt. Bij 21% ging het zelfs om een aanzienlijke aanscherping. Meest genoemde reden is verandering van de wetgeving. Denk aan de Wet Bescherming Persoonsgegevens en de Meldplicht Datalekken. Andere redenen zijn de nieuwe eisen op het gebied van informatieveiligheid, die gesteld worden bij ISO-certificatie.

Ook de overstap naar de cloud leidt tot veranderingen in het veiligheidsbeleid. Overheden verwijzen onder meer naar decentralisaties in het Sociaal Domein en de Baseline Informatiebeveiliging Gemeenten. Zorgverleners noemen NEN 7510.

Op organisatorisch gebied is ook veel ondernomen. Men maakt gewag van nieuwe stuurgroepen, monitoring van informatiegebruik en projecten gericht op het vergroten van veiligheidsbewustzijn. Verder worden medewerkers strakker aangestuurd op bestandsbeveiliging met wachtwoorden, gaat men over op encryptie van berichten of worden gedragscodes geformuleerd voor het gebruik van sociale media.

Op technologisch gebied voert men een strakker beheer voor mobile devices en komen er richtlijnen rond het gebruik van USB-sticks. Deze mogen bijvoorbeeld niet direct in het zicht liggen en moeten na gebruik geleegd worden. Verder mogen medewerkers bij een aantal organisaties geen bestanden meer opslaan op laptops, zijn e-mails alleen via een centraal archief in te zien of heeft men een portaal ingericht voor gegevensuitwisseling (in plaats van documenten te mailen). En uiteraard worden de firewalls steeds verder opgehoogd.
Ruim een kwart van de organisaties heeft de veiligheidszaken op orde of ziet geen aanleiding het beleid te veranderen en 6% geeft aan dat er geen beleid is voor informatieveiligheid. Dat laatste is uiteraard zorgelijk.

Wat is er veranderd in het beleid rond informatieveiligheid in de afgelopen 12 maanden?



Veranderingen op basis van nieuwe wet- en regelgeving

Nationale en Europese wet- en regelgeving, maar ook richtlijnen vanuit branches, maken het speelveld van informatieveiligheid enorm divers en complex. Iedereen heeft te maken met de Meldplicht Datalekken, deze wordt dan ook door alle deelnemers genoemd als reden voor nieuw beleid. De Wet Bescherming Persoonsgegevens was bij 87% van de deelnemers de reden. NEN-normen (7510 en 7511) waren voor 28% de aanleiding. Verder moet een kwart van de deelnemers zich houden aan de richtlijnen voor de rijksoverheid, zoals deze zijn vastgelegd in de Baseline Informatiebeveiliging Rijksdienst (BIR) en zijn gemeenten gebonden aan de BIG (9%). Het nemen van de eigen verantwoordelijkheid wordt door 3% van de deelnemers aangevoerd. Daarnaast handelt een klein deel van de respondenten proactief of volgt branchespecifieke richtlijnen.

Welke wet- en regelgeving rond informatiebescherming heeft ertoe geleid dat u binnen uw organisatie veranderingen heeft doorgevoerd?

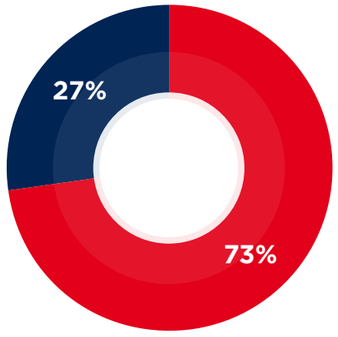
Antwoord	
Meldplicht Datalekken	**100%**
Wet Bescherming Persoonsgegevens	**87%**
NEN7510, NEN7512, NEN7513	**28%**
Overheid BIR / NEN ISO 27001/27002	**25%**
Anders - ISO15189 - rechtspraak KNB, NOvA - Criteria vanuit de branche - Toetsingskader Informatiebeveiliging DNB - Internationale standaard - ISAE3402 - Europese privacyverordening	**11%**
BIG	**9%**
Deden we al, eigen initiatief (niets veranderd)	**7%**
Latent gevoel dat er iets moet veranderen	**1%**

Verdeeldheid, focus of chaos?

Het MKB weet niet goed raad met de Meldplicht Datalekken

De forse sancties die opgelegd kunnen worden wanneer een datalek niet op de juiste wijze voorkomen en gemeld wordt, heeft bij 27% van de organisaties geleid tot versneld doorvoeren van veiligheidsmaatregelen. Omgekeerd denkt 69% kennelijk dat het zo'n vaart niet zal lopen. Ruim een kwart heeft geen procedure opgesteld voor het geval dat een datalek optreedt en 28% heeft wel een procedure maar die is slechts bij een beperkt aantal medewerkers bekend. Verder heeft 6% geen idee of er een procedure is. Nog geen 40% zegt goed voorbereid te zijn op een datalek. Doorvragen leert dat het MKB wel bekend is met de nieuwe wetgeving, maar niet goed weet wat ze ermee moeten doen, onder meer omdat nog veel onduidelijk is.

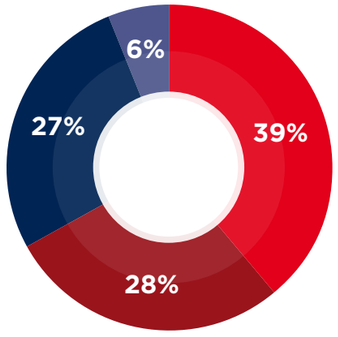
Heeft de dreiging van hoge boetes in het kader van de Meldplicht Datalekken geleid tot het versneld doorvoeren van veiligheidsmaatregelen?



Antwoord

- Nee
- Ja

Heeft u een procedure opgesteld voor het geval een datalek optreedt in uw organisatie?



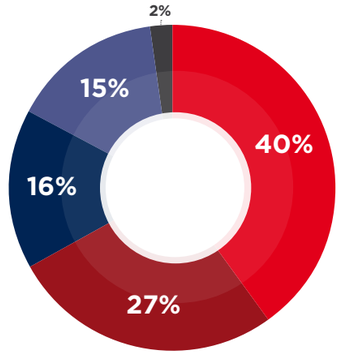
Antwoord

- Ja, wij hebben een procedure en alle medewerkers zijn op de hoogte
- Ja, wij hebben een procedure maar deze is slechts bekend bij beperkt aantal mensen
- Nee, wij hebben geen procedure
- Weet ik niet

Preventie, controle en repressie om gedrag te beïnvloeden

Ook wat informatieveiligheid betreft, is voorkomen beter dan genezen. Daarom hanteert 40% van de organisaties preventieve maatregelen, zoals training en instructie, om te proberen het gedrag van medewerkers te beïnvloeden. Aan de andere kant kiest 27% ervoor om medewerkers te controleren via technische oplossingen of fysieke controle. Dit kan ten koste gaan van hun privacy, waardoor ze misschien ontwijkend gedrag gaan vertonen. Repressieve maatregelen zijn voor 16% van de respondenten de manier om verantwoord gedrag af te dwingen. Nalatigheid wordt hier gestraft.

Welke vorm(en) van maatregelen hanteert u binnen uw organisatie bij het beïnvloeden van het gedrag rond informatieveiligheid?



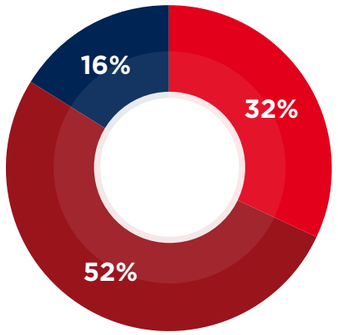
Antwoord

- Preventieve maatregelen (denk aan training en instructie)
- Controlerende maatregelen (bijvoorbeeld monitoring van fysieke werkplekken, remote beheer van laptops en empty desk scans)
- Repressieve maatregelen (sancties bij ongewenst gedrag, denk aan het beperken van autorisaties of noteren van nalatigheden in personeelsdossiers)
- Nog geen maatregelen
- Anders

Gros van de medewerkers weet niet wat informatieveilig werken inhoudt

Dreigen met straffen en op afstand controleren is zinloos als de medewerkers onvoldoende zijn geïnformeerd over het veiligheidsbeleid. Opvallend in dat verband is dat bij 17% van de organisaties medewerkers onvoldoende kennis hebben over de voorschriften met betrekking tot informatieveilig werken. Daarnaast durft 52% hierover geen uitspraak te doen. Als er al een beleid rond informatieveiligheid is, wordt dit dus door gebrek aan concrete kennis vaak niet goed nageleefd.

In hoeverre beschikken alle medewerkers over voldoende kennis over het veilig werken met bedrijfsinformatie en de informatienetwerken op en van het werk en onderweg?

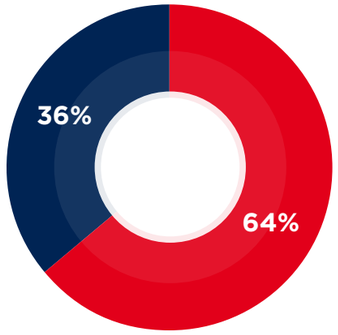


Antwoord
- Volledig
- Neutraal
- Totaal niet

Communicatie over de procedures laat vaak te wensen over

Medewerkers weten meestal niet hoe ze moeten handelen wanneer ze vermoeden dat iemand ongeautoriseerd toegang probeert te krijgen tot het bedrijfsnetwerk of dit al heeft gehad. Bij 64% van de organisaties is hiervoor geen procedure opgesteld. Als er daadwerkelijk privacygevoelige gegevens lekken, dan lijken organisaties onvoldoende voorbereid te zijn om te voldoen aan de Meldplicht Datalekken. Hiernaast zien we dat de opgestelde procedures voor het verhogen van het informatieveiligheidsbewustzijn ook niet altijd goed zijn gecommuniceerd naar alle medewerkers.

Heeft u een procedure uitgerold voor security breach (elke vorm van niet-geautoriseerde toegang) die naar de medewerkers is gecommuniceerd?

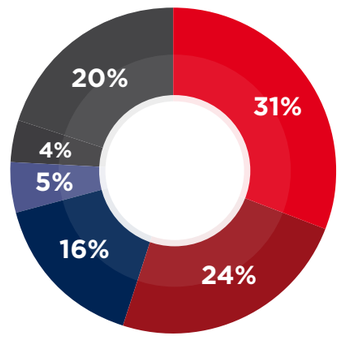


Antwoord
- Nee
- Ja

Werknemers worden op verschillende manieren geïnformeerd

Ongeveer een derde van de organisaties communiceert over de procedures voor informatieveiligheid tijdens reguliere informatiebijeenkomsten. Verder gebruikt 16% training en opleiding voor het instrueren van medewerkers. Ook via toetsing wordt de omgang met informatie beoordeeld: bij 4% jaarlijks en bij 5% doorlopend. In de categorie Anders zien we een verscheidenheid aan middelen. Sommige organisaties communiceren over informatieveiligheid via awareness campagnes, berichtgeving op het intranet, e-mailings of interne nieuwsbrieven. Andere organisaties informeren medewerkers alleen bij indiensttreding of werkoverleg over de procedures. Opvallend is dat bijna een kwart nog niet actief bezig is met kennisoverdracht en bewustwording rond informatieveiligheid.

Hoe worden medewerkers geïnformeerd over de waarde van uw informatienetwerk en de mogelijke impact als informatie in verkeerde handen valt of toegang tot het netwerk gecompromitteerd raakt?



Antwoord
- Via reguliere informatiebijeenkomsten
- Dit gebeurt nog niet, maar zijn we wel van plan binnenkort in te voeren
- Via opleiding en training
- Via doorlopende toetsing
- Via jaarlijkse toetsing
- Anders

Hoe borgen organisaties informatie-veilig werken?

Informatieveiligheid waarborgen vraagt een holistische aanpak. Alle deelnemers zijn het erover eens dat technische oplossingen een must zijn. Maar dat is niet het enige: 87% vindt dat ook procedures en maatregelen nodig zijn. Omgekeerd is 41% van mening dat de medewerkers zelf de verantwoordelijkheid moeten nemen. Als er procedures zijn, moeten medewerkers daarvan uiteraard wel op de hoogte gehouden worden want het informatieveiligheidsdomein is zeer dynamisch. Een derde van de organisaties verzorgt periodiek training en instructie, waarbij 5% dit slechts eenmalig doet bij in dienst treden van medewerkers.

Het is mooi als er procedures zijn opgesteld en er maatregelen worden getroffen. Maar hoe weet men dat de medewerkers ook daadwerkelijk volgens de richtlijnen werken? In hoeverre de kennis is geland en beklijft, wordt slechts bij 6% van de organisaties via een verplichte toets gecontroleerd. Daarnaast controleert 14% steekproefsgewijs het gedrag op de werkvloer en monitort 8% met technische tools hoe de medewerkers handelen. Bewustwordingscampagnes, regelmatige praatsessies en interne audits komen nauwelijks voor.

Kortom, de dynamiek van het digitale veiligheidsdomein zien we nog niet terug in de wijze waarop organisaties hun medewerkers informeren en controleren.

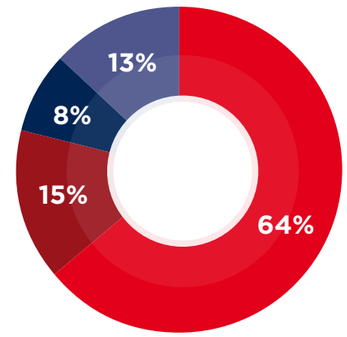
Op welke wijze waarborgt u informatieveiligheid in uw organisatie? (meerdere antwoorden mogelijk)

Antwoord	
Technische oplossingen	100%
Vastgestelde procedures en maatregelen	87%
Medewerkers worden geacht hiervoor zelf verantwoordelijkheid te nemen	41%
Periodieke training / instructie	32%
Eenmalige training / instructie bij in dienst treden van medewerkers	15%
Controle gedrag op de werkvloer (steekproefsgewijs)	14%
Alleen voorlichting en instructies	12%
Monitoring gedrag op afstand (via technische tools)	8%
Verplichte (kennis)toetsing van de medewerkers	6%
Beperkte toegang functiegericht	1%
Bewustwordingscampagne	1%
Frequent communiceren	1%
Interne audits	1%

De rol van externe partijen in het domein van informatieveiligheid

Informatieveiligheid is een domein dat snel verandert en steeds complexer wordt. Er zijn maar weinig mensen die alle facetten volledig in het vizier hebben, weten waar risico's ontstaan en hoe ze die kunnen elimineren. Desondanks kiest 64% van de organisaties ervoor om alleen van externe leveranciers gebruik te maken voor de techniek en niet voor het vergroten van de bewustwording van de medewerkers. Slechts 15% laat ook de training en de monitoring extern verzorgen en 8% de techniek en alleen de training. De 13% die het anders aanpakken, schakelen periodiek externe specialisten in, bijvoorbeeld voor risico- of GAP-analyses en toetsing van de informatieveiligheid. Ook consultancy voor de implementatie van maatregelen wordt genoemd. Het verwachtingspatroon van de rol die leveranciers kunnen vervullen is dus niet eenduidig.

Nu het informatie- en communicatie-speelveld steeds complexer wordt, roepen meer organisaties de hulp in van specialisten. Wat is hun rol bij het beveiligen van alle bedrijfs- en klantinformatie?



Antwoord

- Levert technologie voor autorisatie en databescherming
- Levert techniek, training en monitoring
- Levert technologie en traint medewerkers in veilig omgaan met informatie
- Anders

Hoeveel vrijheid heeft de mobiele werker?
Het feit dat we met zijn allen mobiel zijn gaan werken brengt automatisch met zich mee dat de bedrijfsinformatie gaat reizen. Wat doen organisaties om die reis veilig te maken? Daarbij kan gekeken worden naar netwerken, software en hardware. Waarop zetten organisaties in om werknemers ook thuis en onderweg veilig te laten werken?

Mobiele online toegang
De mobile access provider speelt een primaire rol: 27% van de deelnemers geeft aan dat deze een veilige toegang tot het internet moet garanderen. Bij 6% mogen medewerkers absoluut niet werken via openbare wifispots. Om dat te waarborgen moeten ze uiteraard een abonnement hebben dat overal toegang tot het internet biedt.

Software voor mobile devices
Bij 22% van de organisaties mogen medewerkers alleen software gebruiken die de organisatie beschikbaar stelt. Dat geldt ook als ze met eigen mobiele apparatuur werken. Het is de vraag of medewerkers zich hieraan houden, omdat via het internet allerlei gratis programma's beschikbaar zijn waarmee ze ook privé werken.

Mobiele apparatuur
Bij 17% van de organisaties mogen medewerkers met eigen apparatuur werken, maar alleen als die door de eigen ICT-afdeling is geconfigureerd en beveiligd. Een stap verder gaat de 14% waar werknemers alleen apparatuur mogen gebruiken die door de

Vaak ontbreken procedures over informatieveiligheid of zijn ze niet bij alle medewerkers bekend

Stelling

Moeten IT-leveranciers ook veilig informatiegedrag bevorderen?
In de benchmark was de volgende stelling opgenomen:

> *Leveranciers van software- en hardwarematige oplossingen rond informatieveiligheid dienen naast het leveren van de oplossing ook een rol te spelen bij het beïnvloeden en sturen van veilig informatiegedrag door medewerkers.*

Deze stelling wordt door 77% onderschreven. Dit is opvallend, omdat eerder is aangetoond dat opgeteld slechts 21% van de respondenten leveranciers inschakelt voor training en monitoring en 64% alleen de technische oplossing afneemt. Voorstanders van de stelling vinden het gedrag van medewerkers allesbepalend voor succes van informatiebeveiligingsbeleid. Anders zijn maatregelen zinloos.

Een greep uit de reacties:

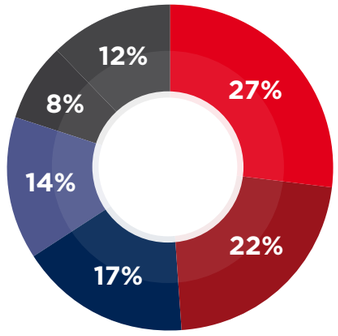
- *Medewerkers moeten zowel de technologische oplossing adopteren als een hogere attentiewaarde hebben met betrekking tot informatieveiligheid. Het is goed dat de leverancier de klant attendeert op de mogelijkheden om trainingen en cursussen mee te nemen in het veranderingsproces.*
- *Bewustwording vormt een zeer belangrijk onderdeel van informatiebeveiliging en is alleen onder begeleiding van een kundig persoon te realiseren. Leveranciers kunnen hiervoor oplossingen op maat leveren.*
- *De tijd dat het alleen om software of hardware appliances ging, ligt ver achter ons. Vandaag de dag ligt de focus op begeleiding van eindgebruikers.*
- *Een technische oplossing verhelpt geen mentaliteitsprobleem van medewerkers met betrekking tot informatieveiligheid.*
- *Gedrag is allesbepalend voor het succes van informatiebeveiligingsbeleid. Als je gedrag niet in positieve zin beïnvloedt, is de rest van de genomen maatregelen kansloos. Laat medewerkers nut en noodzaak inzien van te nemen maatregelen.*
- *Leveranciers moeten zich bewust zijn van de gevolgen die het gebruik van programma's en hardware hebben en de manier waarop medewerkers hiermee omgaan.*
- *Een leverancier weet als geen ander waar en hoe het fout kan gaan en geeft daar, als het goed is, gericht advies over.*

organisatie wordt aangeboden. We spreken in dit verband van Choose Your Own Device (CYOD) en Company Owned, Personally Enabled (COPE).

Andere security solutions

Hoe houdt de 12% die Anders geantwoord hebben het mobiel werken veilig? Onder meer overheden noemen het faciliteren van ‘containerized’ werken. Medewerkers mogen dan hun eigen device gebruiken, maar bedrijfsinformatie wordt ‘verpakt en verzegeld’ aangeboden middels een streng beveiligde app. Hierdoor zijn bedrijfsgegevens zelfs niet toegankelijk bij het hacken van een smartphone. Andere genoemde methoden zijn Virtual Desktop Infrastructure (VDI) met sms-authenticatie, Citrix (thin clients), inlog op afstand met beveiligde USB-sticks en VPN-tunnels voor remote access. Er zijn ook organisaties die niet aan beveiliging doen of dit aan de medewerkers overlaten.

Mobiel werken brengt risico’s met zich mee. Welke maatregelen heeft u genomen om te zorgen dat uw medewerkers onderweg en thuis veilig werken?



Antwoord

- Onze provider biedt mobiele werkers een beveiligde toegang
- Medewerkers mogen alleen software gebruiken die de organisatie beschikbaar stelt
- Er mag met eigen mobiele apparatuur gewerkt worden als deze is geconfigureerd en beveiligd door ICT
- Er mag alleen gewerkt worden op apparatuur die door de organisatie wordt aangeboden
- Er mag niet gewerkt worden vanaf publieke wifispots
- Anders

Vraag

Belang van informatieveiligheid voor de reputatie

In het onderzoek was de volgende vraag opgenomen:

> *Als informatieveiligheid in het geding komt, wat betekent dit dan voor het vertrouwen in de relatie met klanten, leveranciers en andere belanghebbenden?*

De respondenten zijn met name bang voor beschadiging van de reputatie omdat die niet te begroten is en organisaties ernstige schade kan berokkenen. Dat geldt met name voor gemeenten, financiële dienstverleners en zorginstellingen die veel privacygevoelige informatie hebben opgeslagen.

Wat zal er gebeuren bij een datalek of security breach?

Een greep uit de reacties:

- *Burgers moeten erop kunnen vertrouwen dat de overheid hun persoonlijke, vertrouwelijke en gevoelige informatie beschermt. Daarom zetten we hier maximaal op in.*
- *Als gegevens op straat komen te liggen, krijgt het vertrouwen een deuk en hebben we heel wat uit te leggen aan onze klanten.*
- *De praktijk wijst uit dat wanneer een incident heeft plaatsgevonden, het niet meer gaat om rationele feiten maar om beeldvorming waarbij geen plaats is voor nuance. Achteraf uitleggen dat het echt goed was geregeld, wordt geïnterpreteerd als ontkenning en werkt wellicht zelfs averechts. Vertrouwen komt te voet en gaat te paard.*
- *Binnen de juridische dienstverlening kan men zich geen fouten veroorloven. Dit zal blijvende imago-schade opleveren.*
- *Het maakt natuurlijk uit welke informatie het betreft. Als bijvoorbeeld patiënten/cliënten-dossiers publiek worden gemaakt zal dit het vertrouwen in onze organisatie ernstig schaden.*

Hoofdstuk 04

Conclusies en aanbevelingen

Eindconclusies

- Organisaties denken dat het veiligheids-risico van buiten komt, maar in de praktijk komt dit voornamelijk van binnen de organisatie.
- Slechts een vijfde van de medewerkers voelt zich verantwoordelijk voor informatie-veiligheid.
- Informatieveiligheid is een steeds complexer domein waarvan het management vaak nog in de kinderschoenen staat. ICT is traditioneel in de lead, maar het merendeel van de deelnemers meent dat met alleen technologische oplossingen de informatieveiligheid niet gewaarborgd kan worden. De mens-kant (HR) is minstens zo belangrijk. Dit onderzoek heeft nader gekeken naar bewust-zijn en gedrag: diepgaandere aspecten vanuit de mens-kant. Het blijkt dat veel mensen nog onbewust onbekwaam met informatie omgaan.
- Het grootste risico vormt volgens de respondenten het feit dat informatie fysiek rondslingert. Denk aan memostickers en bureauleggers met aantekeningen, documenten die niet van de printer worden gehaald of USB-sticks die in een computer worden achtergelaten. Er is meer veiligheidsbewustzijn nodig om dit symptoom, dat we in het onderzoek ‘zwerf-informatie’ noemen, te voorkomen.
- Mensen nemen hun gedrag als informatie-consument mee naar het werk. Ze willen zakelijk net zo makkelijk kunnen communiceren en informatie uitwisselen als in hun privésituatie. Denk aan het gebruik van sociale media, WhatsApp, Dropbox en Gmail. Dit consumentisme creëert grote veiligheidsrisico’s wanneer werknemers zich niet bewust zijn van de informatie die ze prijsgeven. Bestanden, zoals digitale documenten, zijn net water: ze zoeken altijd de weg van de minste weerstand. Daarbij zijn mensen niet bewust van het informatie-spoor dat ze achterlaten.
- Het bewustzijn van de waarde van privacy- en concurrentiegevoelige informatie is schrikbarend laag.
- De verantwoordelijkheid voor informatie-veiligheid wordt op verschillende plaatsen in organisaties belegd. Soms stelt men de medewerker zelf verantwoordelijk. Het besef dringt nog niet of nauwelijks door dat informatieveiligheid een gemeen-schappelijke verantwoordelijkheid is van de organisatie (processen, techniek, regels, voorlichting) en alle medewerkers.
- De complexiteit en de dynamiek van het vraagstuk ‘informatieveiligheid’ maakt dat er wel over gesproken wordt, maar dat er in veel organisaties nog geen strak beleid is uitgezet. Werknemers worden op verschillende manieren geïnformeerd: bijna een kwart van de bedrijven is nog niet actief bezig met bewustzijnsontwikkeling. Het gros van de medewerkers weet niet wat informatieveilig werken inhoudt: men kent het beleid niet. Communicatie over de procedures laat vaak te wensen over, omdat procedures vaak ontbreken. Dit is alarmerend!
- Bij slechts een beperkt aantal organisaties - vooral de grote ondernemingen - hebben informatieveiligheidsspecialisten hun intrede gedaan. Er wordt nog relatief weinig gebruik gemaakt van externe partijen voor training

en monitoring van de veiligheidssituatie. Dat is opvallend omdat het gros van de respondenten meent dat de IT-leverancier hierin een rol zou moeten spelen.
- Tot slot loopt het tempo van de ontwikkelingen van het veiligheidsbewustzijn nog niet synchroon met de technologische ontwikkelingen. Informatieveiligheid is een groot vliegwiel dat langzaam op gang komt. Veel organisaties bevinden zich nog in de beginfase van de weg naar bewustzijnsverandering. Het gedrag van medewerkers is van kritisch belang voor het succes van een informatiebeveiligingsbeleid. Het gaat om een holistische aanpak.

Aanbevelingen

Zwerfinformatie is een symptoom van de manier waarop mensen met informatie omgaan. Je kunt zwerfinformatie bestrijden als goed in kaart is gebracht welke informatie geen plek heeft binnen de primaire processen en derhalve op allerlei plekken bewaard wordt, zoals laptops, USB-sticks, bureaus en de toegankelijke 'public cloud storage' platformen zoals Dropbox, WeTransfer en Google Drive.

Zwerfinformatie hoeft niet altijd erg te zijn. Dat wordt het pas als de veiligheid in het geding komt, bijvoorbeeld als het gaat om privacygevoelige informatie.

- Begin bij de technologische kant van de informatieveiligheidsdriehoek. Wat zijn de reeds aanwezige softwarepakketten of -applicaties en welke mogelijkheden worden daarbinnen geboden voor optimalisatie van werkprocessen en het invullen van specifieke behoeftes van medewerkers?
- Het gedrag van mensen en de zogenaamde 'workarounds' die gecreëerd worden rondom bestaande applicaties is een tweede aspect. Zijn die er, waarom doen medewerkers dit, wat zijn de risico's?
- Neem hier parallel in mee of medewerkers bewust met informatieveiligheid bezig zijn.
- Wie initieert het informatieveiligheidsbeleid? Wie is waar verantwoordelijk voor als er iets mis gaat? Naast helder communiceren wat wel en niet mag, zijn er ook vele interessante trainingen of seminars beschikbaar waarin medewerkers geïnformeerd worden over de risico's van zwerfinformatie.
- Als blijkt dat de mogelijkheden van bestaande softwarepakketten uitgeput zijn, of als aanpassingen en/of toevoegingen niet efficiënt toegepast kunnen worden om te voldoen aan de behoefte van de medewerkers, is het interessant om te gaan kijken welke additionele software wel kan voorzien in deze behoefte.
- Zwerfinformatie als symptoom bevindt zich ook aan de outputkant, het 'einddocument', zoals de print, de factuur of aantekeningen op flipovers. Dit is vrij eenvoudig op te lossen door bijvoorbeeld een printmanagementbeleid in te stellen.
- Krijg "zonder omwegen goed en veilig werken met informatie" op de agenda van de gehele organisatie. Informatiebeveiliging is niet alleen ICT-security, daar komt veel meer bij kijken. Het is een zaak van de gehele onderneming, van hoog tot laag. Een speciale functionaris gegevensbescherming (FG) oftewel data protection officer (DPO) kan een spin in het web zijn om iedereen in de organisatie, van hoog tot laag, bewust te maken, te trainen en te auditen.
- Bepaal tot op welk niveau de verschillende informatie beschermd moet worden. Kroonjuwelen verdienen een ander informatiebeleid en daarmee een ander beschermingsniveau dan gegevens die openbaar beschikbaar mogen zijn. Kijk naar de kosten en baten.

Over Veenman

Veenman is een onafhankelijke partner die organisaties helpt grip te krijgen op hun informatie-voorziening. Met een breed scala aan oplossingen – van printing en document management software tot videoconferencing en interne zoekmachines - zorgt Veenman ervoor dat werknemers informatie in de hand krijgen voor het nemen van beslissingen. Naast het hoofdkantoor in Rotterdam heeft Veenman vestigingen in Amsterdam, Best en Zwolle. De onderneming maakt deel uit van Xerox Corporation. Voor meer informatie: www.veenman.nl

Postbus 1302
3000 BH Rotterdam
Linatebaan 101
3045 AH Rotterdam

T 010 284 6123
F 010 284 6177
www.veenman.nl
info@veenman.nl

veenman

INFORMATIE IN DE HAND