SOPHOS
Security made simple.

Rapport

Onderzoek Encryptie Publieke Sector

Oktober 2015

Contents

Achtergrond van het onderzoek

Aanleiding onderzoek

Encryptie, het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden, is geen vrijblijvende zaak meer, maar bittere noodzaak.

Zowel op internationaal als op nationaal niveau, bevindt wetgeving rondom encryptie zich in een vergevorderd stadium. Zo is in Nederland op 10 februari jongstleden het wetsvoorstel Meldplicht datalekken door de Tweede Kamer goedgekeurd. Het doel van de voorgestelde wet is het voorkomen van datalekken en, mocht er toch gelekt worden, de effecten ervan te beperken. Iedereen moet er namelijk op kunnen vertrouwen dat zijn/haar persoonsgegevens voldoende beveiligd worden.

De vraag is echter hoe het staat met de bewustzijn rondom informatiebeveiliging bij overheden en andere non-profit-instanties. zake gegevensbescherming.

Sophos heeft daarom een online kwantitatief onderzoek uitgevoerd onder mensen die werkzaam zijn in de tertiaire dienstverlening en welke (mede) beslisser zijn op het gebied van IT zaken of een ICT-functie vervullen.

Doelgroep

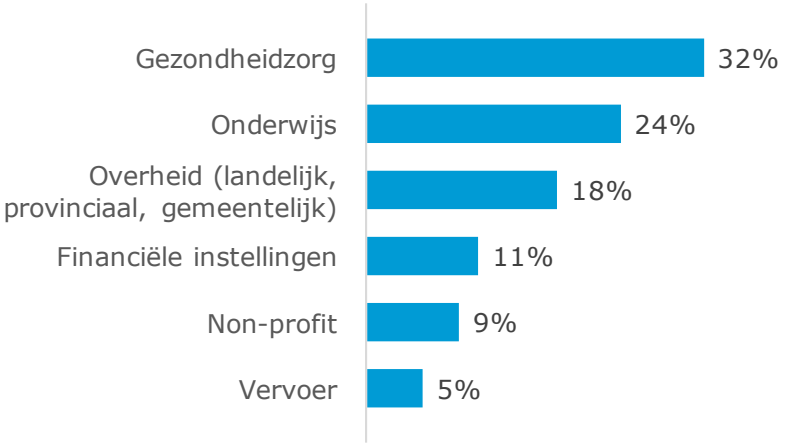
De doelgroep van het onderzoek bestaat uit de 262 IT (mede-) beslissers en ICT'ers binnen de volgende sectoren:

- Gezondheidszorg
- Onderwijs
- Overheid
- Financiële instellingen
- Non-profit
- Vervoer

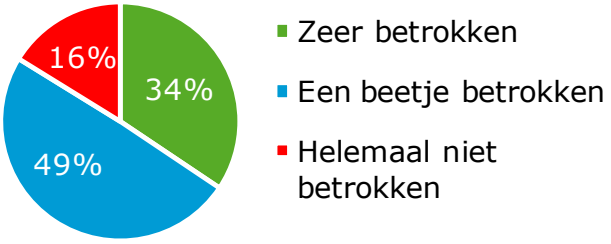
Doelgroep van het onderzoek

Een grote meerderheid van de ondervraagden is betrokken bij het IT-beleid. De IT'ers in het onderzoek komen vooral uit de (semi-)publieke sector: een derde uit de gezondheidszorg en een kwart uit het onderwijs.

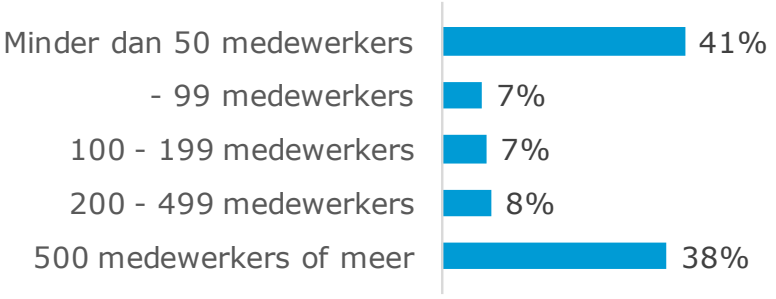
Branche



Betrokkenheid IT-beleid



Bedrijfsgrootte



Vraag: In welke van de onderstaande branches bent u werkzaam?| n=262
Vraag: Wat is uw bedrijfsgrootte?| n=262
Vraag: In hoeverre bent u betrokken bij de totstandkoming van het IT-beleid? | n=262

Samenvatting / Conclusies

Informatiebeveiliging en encryptie zijn begrippen die zeer in de schijnwerpers staan door het stijgen van de privacy inbreuken en EU-wetgeving inzake gegevensbescherming. De resultaten uit dit onderzoek laten zien dat er nog slagen te maken zijn in zowel beleidsbepaling als bewustzijn rondom informatiebeveiliging in de publieke sector.

BEWUSTZIJN

Een van de grootste veranderingen die zich volgens IT'ers de laatste jaren heeft voltrokken met betrekking tot het werken in IT is het toegenomen bewustzijn van gegevensbeveiliging, onder andere door de nieuwe wetgeving.

Toch is lang niet iedereen op de hoogte van de recente wetgeving rondom de meldplicht van datalekken. Meer dan de helft weet hier helemaal niet vanaf; een derde is er een beetje van op de hoogte. Informatie rondom dit onderwerp komt vooral tot de IT'ers via het eigen netwerk en in mindere mate via de media.

De meerderheid van de organisaties die op de hoogte is van deze wetgeving omtrent datalekken is ook van plan hiervoor actie te ondernemen, waarbij vaak de afdeling IT in de lead is.

IT-BELEID

De meerderheid (70%) van de organisaties in de onderzochte sectoren heeft een IT-beleid. Vooral in de overheidssector heeft bijna elke organisatie een IT-beleid, terwijl dit in de non-profit en gezondheidszorg veel lager is.

Het personeel is ook vaak op de hoogte van het IT-beleid, wanneer deze aanwezig is. In de helft van deze gevallen wordt dit ook gemonitord.

BEVEILIGING

Er komen drie voorname zorgen naar voren omtrent IT-beveiliging: verlies van data, gerichte aanvallen en cybercriminaliteit. Driekwart van de IT'ers is van mening dat de huidige IT-security voldoende bescherming biedt tegen deze problemen, hoewel er bij veel organisaties nog verbetering mogelijk is.

Iets meer dan de helft van de organisaties maakt zowel gebruik van Endpoint als Network security. 1 op de 10 geeft aan helemaal geen beveiliging te hebben. In de gezondheidzorg ligt dit percentage met name hoog; 24% heeft geen beveiliging.

On-premise is de voornaamste locatie voor de IT-Security. Het ligt niet in de lijn der verwachtingen dat veel organisaties de locatie van hun IT-Security op korte termijn zullen veranderen.

Meerderheid IT-managers publieke sector kent meldplicht datalekken niet

Nieuwe richtlijn per 2016 heeft grote gevolgen voor IT-beleid en gegevensbeveiliging

Over iets meer dan twee maanden gaat de meldplicht datalekken in die organisaties verplicht om datalekken direct te melden, op straffe van hoge boetes. Uit onderzoek in opdracht van Sophos blijkt dat een ruime meerderheid van de IT-managers die bij overheid en instellingen betrokken zijn bij het IT-beleid, niet op de hoogte is van de invoering van de meldplicht. Volgens IT-beveiliger Sophos zou de overheid een veel prominentere rol moeten spelen bij het informeren van instellingen en bedrijven over de meldplicht datalekken.

In het onderzoek geeft 58 procent van de 262 ondervraagde IT'ers die bij overheid, in zorg, onderwijs en vervoer en bij financiële instellingen verantwoordelijk zijn voor de IT aan dat ze niet op de hoogte zijn van de meldplicht datalekken. Van de overige 42 procent zegt 49 procent via het eigen netwerk en 37 procent via de media geïnformeerd te zijn. 29 procent van de organisaties die de meldplicht kennen heeft actie ondernomen, 44 procent is van plan dit nog te doen, 15 procent heeft geen plannen, 13 procent weet niet wat de plannen van de organisatie zijn. De afdeling IT moet het voortouw nemen bij eventuele acties, zegt een derde (35 procent) van de organisaties die de meldplicht kennen. Een kwart (26 procent) vindt dat de bal bij het managementteam of de bestuurders ligt, een kleiner percentage noemt een speciaal projectteam (11 procent) of de juridische afdeling (10 procent).

Meldplicht bij Autoriteit Persoonsgegevens

Met ingang van 1 januari 2016 zijn bedrijven, instellingen en overheden in Nederland verplicht om inbreuken op de IT-beveiliging te melden bij de Autoriteit Persoonsgegevens – vanaf volgend jaar de nieuwe naam van het College bescherming persoonsgegevens (CBP) - die leiden tot bijvoorbeeld diefstal, verlies of misbruik van persoonsgegevens. De meldplicht datalekken is een uitbreiding van de Wet bescherming persoonsgegevens (Wbp). Boetes voor het niet naleven van de meldplicht kunnen oplopen tot 810.000 euro of 10 procent van de jaaromzet.

Een taak van de overheid

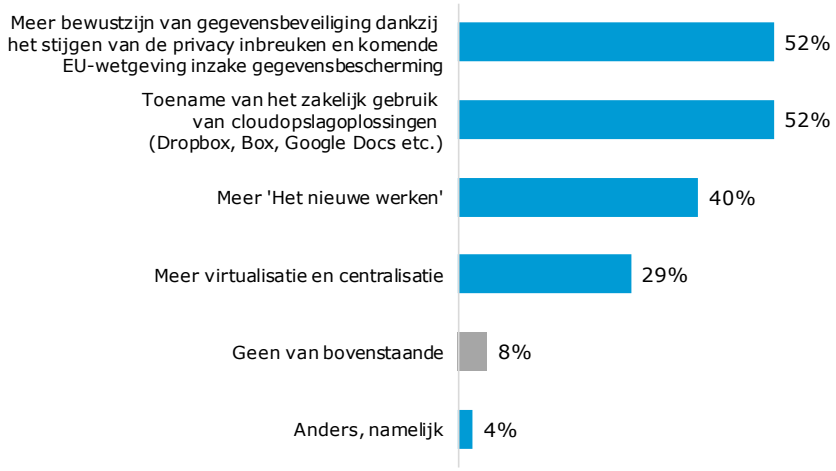
Pieter Lacroix, managing director van Sophos Nederland, is verbaasd maar niet verrast over de geringe bekendheid van de meldplicht datalekken. "Wij merken dat veel organisaties de nieuwe richtlijn niet kennen. Ze schrikken wel als ze van ons horen wat de meldplicht inhoudt en wat de consequenties kunnen zijn van het niet naleven van de regels. Het verbaast me dat er niet veel meer aandacht aan besteed wordt. De overheid moet hier volgens mij veel meer ruchtbaarheid aan geven. Richting consumenten die meer rechten krijgen, maar ook richting Nederlandse bedrijven en instellingen die serieus aan de slag moeten met beveiliging en versleuteling van gegevens. Een eventuele sanctie kan namelijk het voortbestaan van een organisatie in gevaar brengen."

Ook Europese wetgeving wordt strenger

Uit het onderzoek in opdracht van Sophos blijkt wel dat ruim de helft van de ondervraagden gegevensbeveiliging een van de belangrijkste onderwerpen vindt voor het IT beleid, vanwege de toename van het aantal inbreuken op de bescherming van persoonsgegevens en de aanscherping van de EU-privacyrichtlijnen. Volgend jaar wordt naar verwachting ook de nieuwe Europese privacyrichtlijn (GDPR) van kracht.

Manier van werken

Volgens meer dan de helft van de IT'ers is een van de belangrijkste veranderingen in de sector het verhoogde bewustzijn van beveiliging door onder andere de komende EU-wetgeving. Vooral binnen de overheid is dit het geval.



Overheid	Gezondheidzorg	Onderwijs
65%	49%	44%
33%	46%	73%
67%	25%	31%
48%	19%	25%
2%	12%	8%
6%	4%	5%

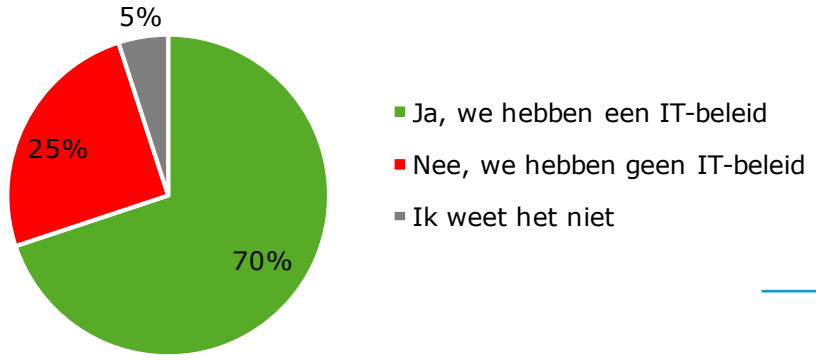
Vraag: De volgende vragen hebben betrekking op IT-security en beleid. De manier van werken is in de afgelopen 2-3 jaar aanzienlijk veranderd. Wat zijn volgens u de grootste veranderingen met betrekking tot IT geweest? n=262

IT Beleid

IT-beleid binnen organisatie

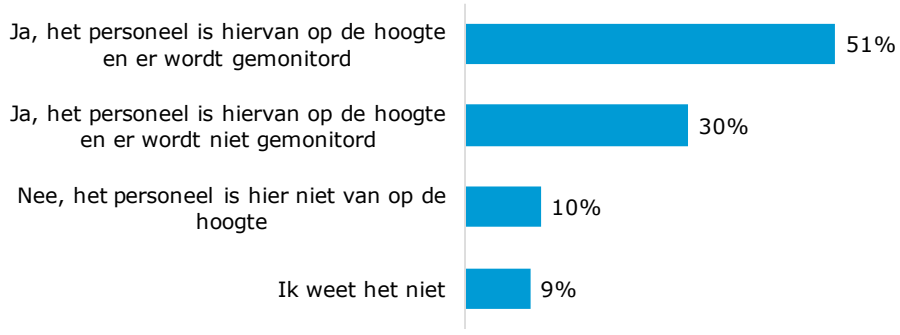
In 70% van de organisaties is sprake van een IT-beleid, waar het personeel ook vaak van op de hoogte wordt gesteld. In de Non-profit sector en de gezondheidszorg ligt dit echter een stuk lager, terwijl de overheidsorganisaties juist vaak een IT-beleid hebben.

IT-beleid organisatie



Non-profit	57%
Gezondheidzorg	40%
Vervoer	21%
Financiële instellingen	18%
Onderwijs	14%
Overheid	2%

Op de hoogte IT-beleid



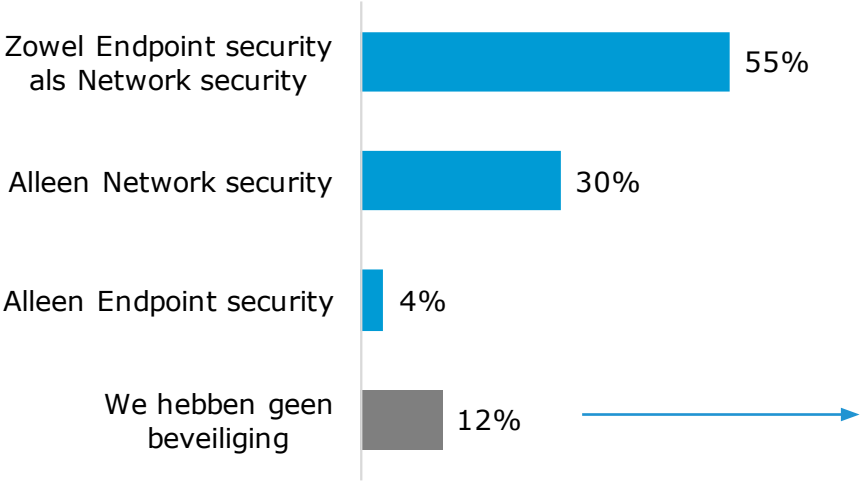
Vraag: Heeft uw organisatie een IT-beleid? | n=262

Vraag: Is het personeel op de hoogte van het IT-beleid, en wordt dit gemonitord?| n=197

Inrichting IT-security

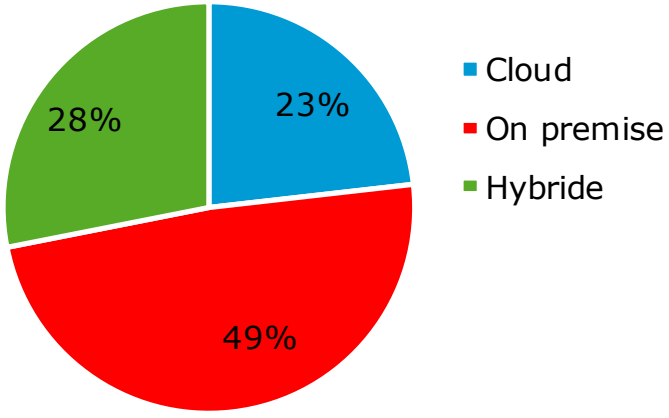
De meeste organisaties maken gebruik van zowel endpoint als network security, welke zich in de helft van de gevallen on premise bevindt. In de gezondheidszorg heeft een kwart echter geen IT-beveiliging.

Inrichting IT-security



Gezondheidzorg	24%
Non-profit	13%
Onderwijs	11%
Financiële instellingen	4%
Vervoer	0%
Overheid	0%

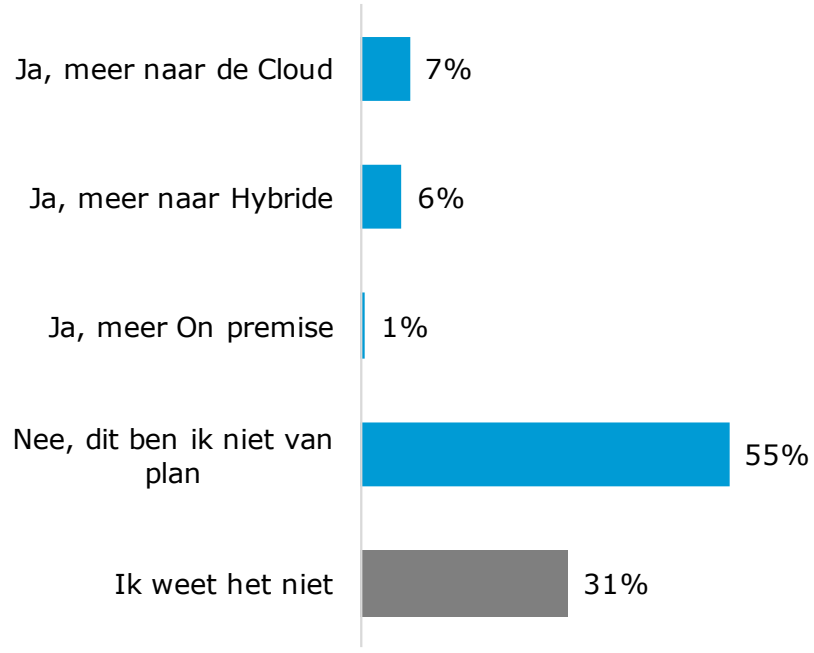
Locatie IT-security



Vraag: Hoe heeft u uw IT-security ingericht? | n=262
Vraag: Waar bevind uw IT-security zich? | n=231

Veranderen IT-security

De meeste organisaties zijn niet van plan om de locatie van hun beveiliging te wijzigen. Vooral in Zuid-Nederland is men van plan de locatie gelijk te houden op korte termijn.



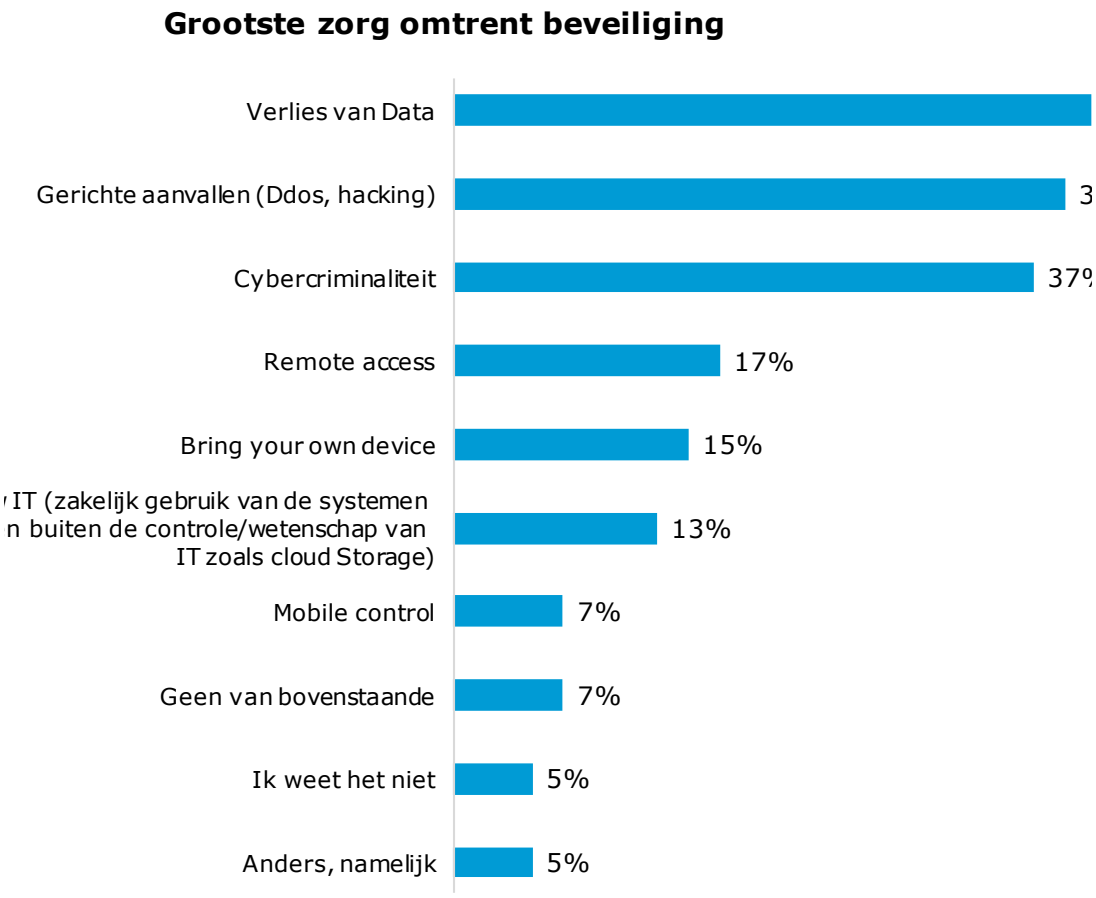
Zuid NL	63%
West NL	55%
Oost NL	50%
Noord NL	46%

Vraag: Bent u op korte termijn van plan de locatie van uw IT-security te veranderen? | n=262

Cybercriminaliteit

Grootste zorg omtrent beveiliging

Er zijn drie grote zorgen omtrent beveiliging: verlies van data, gerichte aanvallen en cybercriminaliteit. Nieuwe ontwikkelingen als BYOD roepen (nu nog) minder zorgen op.

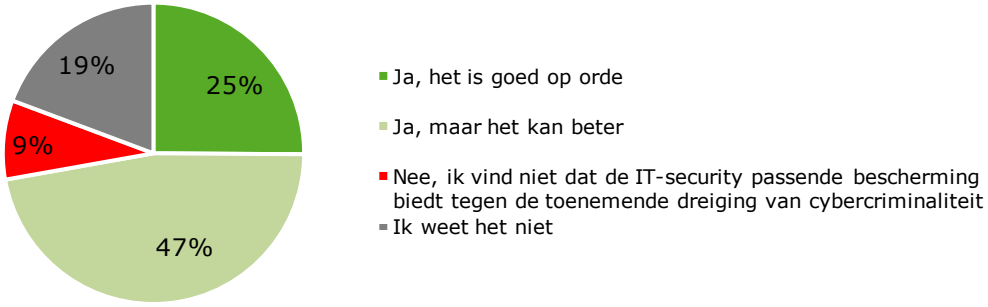


Vraag: Wat is volgens u de grootste zorg als het gaat om de beveiliging van de IT binnen uw organisatie? | n=262

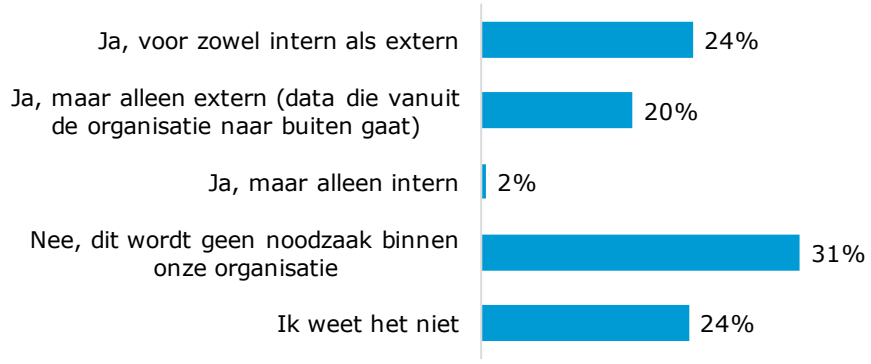
Bescherming

Bijna driekwart van de IT'ers vindt dat zijn huidige IT-security een passende bescherming biedt tegen cybercriminaliteit. De noodzaak voor encryptie is met name hoog binnen de overheidssector; hier geeft 48% aan dat encryptie zowel voor intern als extern gebruik noodzakelijk is.

Bescherming cybercriminaliteit



Noodzaak encryptie



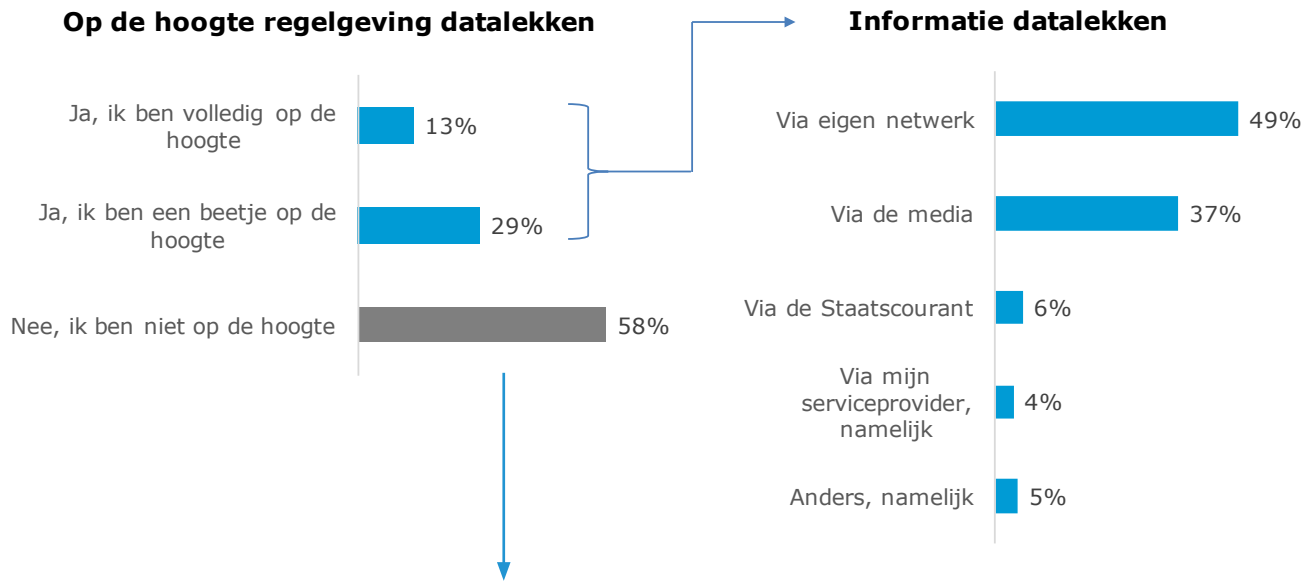
Overheid	48%
Financiële instellingen	32%
Gezondheidzorg	18%
Non-profit	17%
Onderwijs	16%
Vervoer	14%

Vraag: Vindt u dat uw huidige IT-security passende bescherming biedt tegen de toenemende dreiging van cybercriminaliteit? | n=262

Vraag: Wordt encryptie steeds meer een noodzaak binnen uw organisatie?| n=262

Meldplicht datalekken – 1

Ruim de helft van de IT'ers is niet op de hoogte van de regelgeving omtrent meldplicht datalekken. Met name in de sectoren non-profit en onderwijs ligt dit percentage hoog.



West NL	63%
Oost NL	56%
Noord NL	54%
Zuid NL	54%

Non-profit	74%
Onderwijs	67%
Gezondheidzorg	62%
Vervoer	50%
Overheid	44%
Financiële instellingen	43%

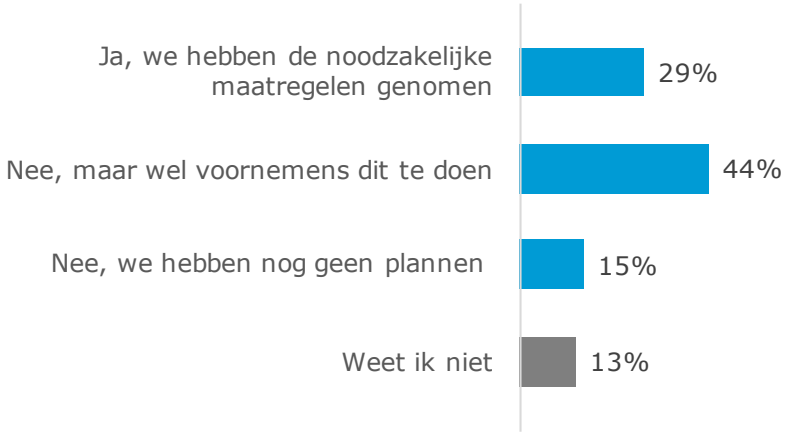
Vraag: Bent u op de hoogte van de komende regelgeving omtrent meldplicht datalekken?| n=262

Vraag: U heeft aangegeven (een beetje) op de hoogte te zijn van de komende regelgeving omtrent de meldplicht datalekken, hoe bent u hierop gewezen? | n=109

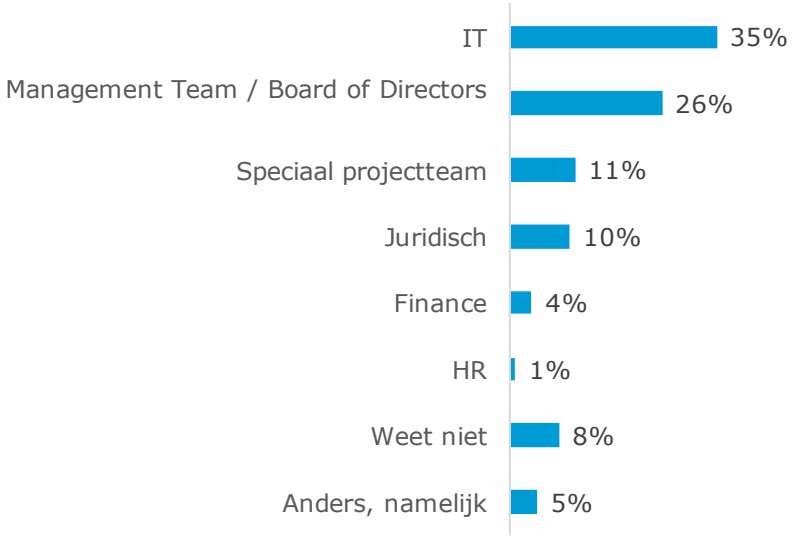
Meldplicht datalekken – 2

In de meerderheid van de organisaties waar men bewust is van de komende wetgeving is of wordt ook hieromtrent actie ondernemen. IT is vaak in de lead over dit onderwerp; in de sector overheid is de juridische afdeling hier ook vaak voor verantwoordelijk.

Actie regelgeving



Afdeling in lead



Overheid	Gezondheidzorg	Onderwijs
30%	28%	38%
26%	28%	38%
7%	16%	5%
22%	3%	5%
4%	0%	0%
0%	0%	0%
7%	16%	10%
4%	9%	5%

Vraag: Heeft u naar aanleiding hiervan actie ondernomen? | n=109
Vraag: Welke afdeling draagt hierin de lead? | n=109

Over Sophos

Meer dan 100 miljoen gebruikers in 150 landen rekenen op Sophos voor de beste bescherming tegen complexe bedreigingen en dataverlies. Sophos levert security- en databeschermingsoplossingen die eenvoudig in te zetten, te beheren en te gebruiken zijn. Zo biedt Sophos prijswinnende oplossingen aan voor endpoint security, web security, e-mail security, network security, mobile security, cloud security en encryptie. Deze worden ondersteund door Sophos Labs, een wereldwijd netwerk van threat intelligence centra. Het hoofdkwartier van Sophos bevindt zich in Oxford (UK). Meer informatie over Sophos op: www.sophos.com.

Oxford, UK | Boston, USA

2015.12.15 R-NA (RP)