



RAPPORT
MKB ONDERZOEK
NEDERLAND EN BELGIË

24 juni 2003

Symantec Benelux
Tav: M. Monasso
Schipholweg 119
2316 XC Leiden



Disclaimer: Alle conclusies, adviezen en/of aanbevelingen, dan wel passages in dit onderzoeksrapport die een adviserend karakter hebben, zijn naar beste weten en kunnen gegeven.

Morph Research heeft werkzaamheden verricht en/of adviezen gegeven op basis van door opdrachtgever aangegeven randvoorwaarden en heeft hierbij gebruik gemaakt van informatie/producten verkregen van opdrachtgever en/of derden. Op basis van andere factoren en gegevens die niet in het onderzoek betrokken zijn, kan een andere conclusie, advies en/of beslissing opportuun zijn. Over de informatie/producten verkregen van opdrachtgever en/of derden heeft Morph Research geen controle en zal derhalve hieromtrent geen enkele aansprakelijkheid aanvaarden.

De resultaten van de werkzaamheden en/of adviezen van Morph Research worden "as-is" geleverd en er kunnen hieraan geen rechten worden ontleend. Morph Research is niet verantwoordelijk en/of aansprakelijk voor schade en/of ander nadeel van opdrachtgever en/of een derde ten gevolge van gebruik en/of openbaarmaking van (delen van) het navolgende onderzoek.

Copyright en auteursrecht berusten uitsluitend bij Morph Research. Openbaarmaking, vermenigvuldiging, verspreiding en/of verstrekking van de informatie in dit document is uitsluitend **toegestaan** met vermelding van de bron.

Morph accountability & research
Vissershavenweg 65-III
2583 DL Den Haag
070-322 69 66



Inhoudsopgave

1. Samenvatting & conclusies	1
2. Beschrijving van het onderzoek	2
2.1 Achtergrond en doelstelling	2
2.2 Methode van onderzoek en doelgroep	2
2.3 Data en rapportage	3
3. Resultaten van het onderzoek	4
3.1 IT-beveiliging	4
3.2 De toekomst	8
3.3 Informatie en verkoopkanalen	9
Bijlagen: - tabellen - vragenlijst	



1. Samenvatting & conclusies

In de periode 13 mei tot en met 13 juni hebben 301 Nederlandse en Belgische Midden en Klein Bedrijven (5-250 werknemers) meegewerkt aan een kwantitatief telefonisch onderzoek. In dit onderzoek, dat in opdracht van Symantec is uitgevoerd, is ondermeer gekeken naar de huidige content- en netwerkbeveiliging van het MKB. De belangrijkste uitkomsten van het onderzoek zijn:

- Veel bedrijven in het MKB besteden de IT-beveiliging uit aan een externe partij. Maar er is ook een grote groep bedrijven waar een werknemer het 'ernaast' doet. Gemiddeld besteden Nederlandse en Belgische bedrijven 8-10% van hun totale budget aan ICT. Een op de tien bedrijven heeft een apart budget voor IT-beveiliging gereserveerd. Dit budget ligt in Nederland op ca. 10% van het totale ICT-budget. In België is dit beduidend lager (4%).
- Uit het onderzoek blijkt dat veel bedrijven beveiligd zijn tegen interne en externe bedreigingen van bedrijfsdata en het netwerk. Slechts 2% van alle bedrijven heeft géén maatregelen getroffen. Antivirus software en firewalls worden relatief het meest gebruikt tegen externe bedreigingen. Nederland loopt in vergelijking met België iets voorop in het gebruik van firewalls, contentfiltering en VPN. Ondanks het gebruik van beveiligingssoftware, heeft een substantiële groep Nederlandse en Belgische bedrijven het idee dat hun netwerk onvoldoende beveiligd is tegen externe bedreigingen (respectievelijk 13% en 25%). Het actualiseren van deze beveiligingssoftware gebeurt vaak automatisch. De frequentie van het actualiseren ligt hoog.
- De belangrijkste kanalen die worden gebruikt om informatie in te winnen over IT-beveiliging zijn internet, de softwareleverancier en IT-bladen. In Nederland spelen verder ook de security consultants een rol in het informatieproces. In België gaat ook de voorkeur uit naar het gebruik van internet. In praktijk blijkt echter dat internet minder wordt gebruikt in vergelijking met Nederland. Dit verschil zou verklaard kunnen worden doordat in Nederland het gebruik van internet al veel meer is ingeburgerd dan in België.
- Circa de helft van alle Nederlandse bedrijven leest wel eens een IT-gerelateerd tijdschrift. In België is dit slechts 38%.
- De verwachting is dat circa één op de zeven bedrijven in Nederland en België de budgetten voor ICT- en IT-beveiliging de komende 6 maanden zal verhogen. De relatief grotere bedrijven tonen de meeste interesse voor nieuwe producten. De interesse in nieuwe software en hardware is het grootst. Bijna één op de vijf bedrijven verwacht dat zij de beveiliging gaan uitbesteden of overweegt zich op een security alert service te abonneren. Eén op de zeven bedrijven toont interesse in anti-spam software. In België tonen vooral de wat kleinere bedrijven interesse in een security alert service.



2. Beschrijving van het onderzoek

2.1 Achtergrond en doelstelling

Symantec, wereldwijd marktleider in Internetbeveiliging, biedt consumenten, bedrijven en service providers een reeks software- en hardwareoplossingen voor content- en netwerkbeveiliging. Symantec biedt voor de zakelijke markt virusbescherming, firewall en virtual private network (VPN), vulnerability management, intrusion detection, Internetcontent- en e-mailfiltering, remote management en security services. Op de consumentenmarkt is Symantec vooral bekend van producten die onder de naam Norton worden aangeboden.

Symantec wil meer inzicht in de huidige content- en netwerkbeveiliging van het Midden en Klein Bedrijf, zowel in Nederland als in België.

De volgende onderzoeksvragen staan hierbij centraal:


- Wat is het toekomstige beleid (budget, personeel etc) tav content- en netwerkbeveiliging
- Welke maatregelen heeft men momenteel getroffen
- Via welke kanalen informeert men zich over IT-beveiliging

2.2 Methode van onderzoek en doelgroep

Het onderzoek is telefonisch uitgevoerd onder MKB bedrijven in België en Nederland met 5-250 werknemers. In Nederland is gebruik gemaakt van het KPN Telecom bestand. In België is gebruik gemaakt van de Belgium Business Directory (infobel.com). Voor de gesprekken met Franstalige bedrijven is gebruik gemaakt van 'native speakers'. De gemiddelde gesprekstijd per interview bedroeg 10 minuten. Het veldwerk vond plaats in de periode 13 mei tot en met 13 juni. Het selecteren en contacteren van respondenten verliep enigszins moeizaam. Dit had vooral te maken met de slechte bereikbaarheid van de bedrijven. Veel tijd is besteed aan het maken van afspraken. Voor het onderzoek is gebruik gemaakt van een Nederlandstalige, Vlaamse en Franstalige vragenlijst. De Nederlandstalige vragenlijst is als bijlage in het rapport opgenomen.

Het onderzoek is afgenomen onder bedrijven die beschikking hebben over internet en/of e-mail. Binnen deze bedrijven is gesproken met personen die (mede) verantwoordelijk zijn voor de ICT/beveiliging. De netto steekproef bedraagt N=301 verdeeld naar N=180 Nederlandse bedrijven (60%) en N=121 Belgische bedrijven (40%).

Respons overzicht	Nederland		België	
	N	%	N	%
Netto respons (geslaagde gesprekken)	180	6	121	8
Objectieve non respons (geen gehoor/niet thuis e.d.)	1315	51	1016	69
Selectieve non respons (weigering)	959	44	286	12
Verkeerd nummer/fax	107	4	144	10
Totaal	2561	100	1567	100



2.3 Data en rapportage

In het rapport zijn de resultaten van Nederlandse en Belgische bedrijven apart geanalyseerd. Daar waar mogelijk zijn uitsplitsingen gemaakt naar bedrijfsgrootte.

In hoofdstuk 2 worden de belangrijkste resultaten van het onderzoek beschreven. De tabellen, en vragenlijst zijn als bijlage toegevoegd.

Voor inhoudelijke vragen over het onderzoek kunt u zich wenden tot Symantec (contactpersoon Mascha Monasso; telnr: 071-408 31 88). Voor onderzoekstechnische vragen kunt u zich wenden tot Morph (contactpersoon Jacques van Leeuwen; telnr: 070-322 69 66).



3. Resultaten van het onderzoek

3.1 IT-beveiliging

Organisatie IT-beveiliging

De internetbeveiliging wordt in veel gevallen uitbesteed aan een externe partij of wordt 'erbij'gedaan door één van de werknemers. Een beperkt aantal bedrijven beschikt zelf over een ICT-afdeling.

Hoe is de ICT/internet beveiliging binnen uw bedrijf georganiseerd?	Nederland	België
Is dat ...	180	121
Basis (100%)=	%	%
Een werknemer doet het erbij	42	51
Er is een ICT afdeling	14	3
Er is één ICT persoon	22	33
Een externe partij (wordt geheel/gedeeltelijk uitbesteed)	34	41
anders	2	2

Budget ICT- en IT-beveiliging

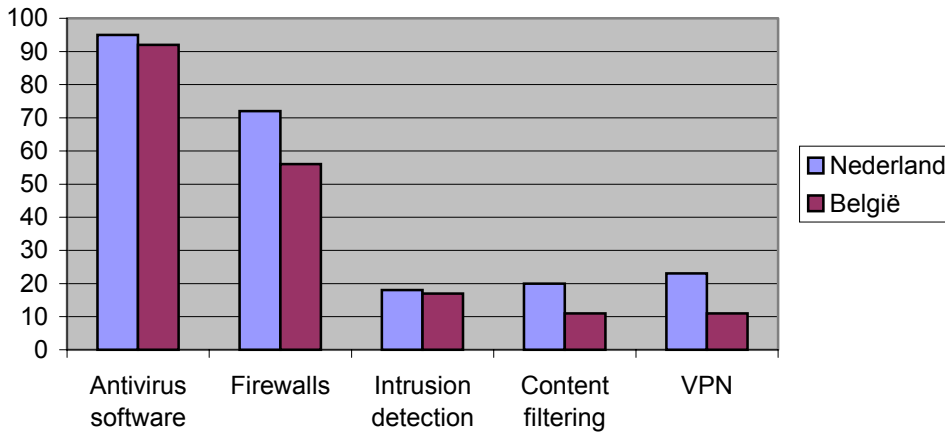
Gemiddeld wordt in Nederland 10% van het totale budget gereserveerd voor ICT. In België ligt dit op 8%. Slechts 10% van alle bedrijven reserveert een apart budget voor IT-beveiliging. Dit zijn vooral de grotere bedrijven (50-250 werknemers). In Nederland ligt dit budget op een niveau van gemiddeld 10%. In België is dit slechts 4% van het totale ICT budget.

	Nederland	België
Basis (100%)=	180	121
	%	%
Gemiddeld budget ICT	10	8
% dat een apart budget heeft voor IT-beveiliging	10	9
Gemiddeld budget IT-beveiliging	10	4



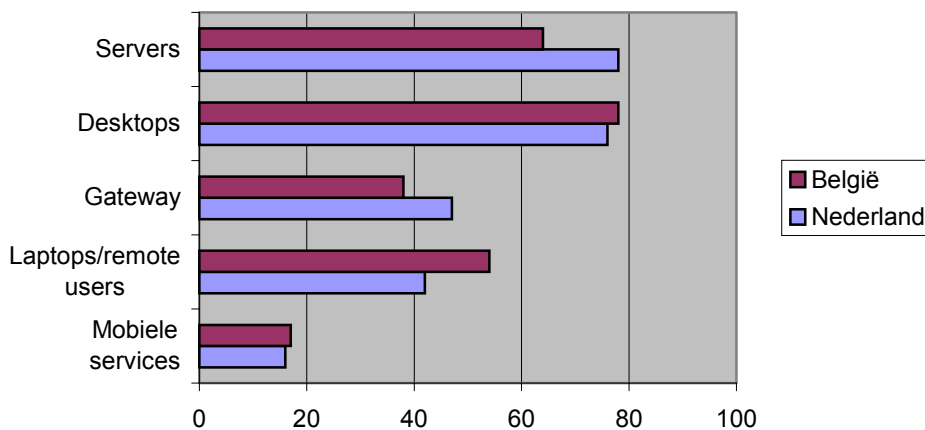
Oplossingen

Aan alle bedrijven is gevraagd welke oplossingen worden gebruikt om hun bedrijfsdata te beveiligen. Slechts 2% heeft geen van onderstaande maatregelen getroffen om de data te beveiligen. Bijna alle bedrijven maken gebruik van antivirus software. Ook firewalls worden door relatief veel bedrijven gebruikt (vooral in Nederland). Over het geheel zien we dat in België de verschillende oplossingen minder vaak worden aangewend om hun data te beveiligen (met uitzondering van antivirus software en intrusion detection).



Onderdelen netwerk

De bedrijven maken vrijwel allemaal gebruik van programma's en applicaties om hun bedrijfsdata te beveiligen (zie paragraaf 'oplossingen'). Aan alle bedrijven is gevraagd welke onderdelen van het netwerk worden beveiligd. De servers en desktops worden in groten getale beveiligd. Ondanks dat de ruime meerderheid van de bedrijven van mening is dat het bedrijfsnetwerk voldoende beveiligd, zijn er toch nog relatief veel bedrijven in Nederland en België die dit niet vinden.



Heeft u het idee dat uw bedrijfsnetwerk voldoende beveiligd is?	Nederland	België
Basis (100%)=	180 %	121 %
Ja	86	75
Nee	13	25



Frequentie bijwerken software

Bij circa de helft van alle ondervraagde bedrijven verlopen de updates van de beveiligingssoftware automatisch en weet men niet aan te geven hoe vaak dit is. Duidelijk is dat de frequentie hoog ligt. Een kwart tot eenderde geeft aan dat de updates 1 keer per maand of vaker gebeuren.

Hoe vaak wordt de <u>software</u> bijgewerkt? Basis (100%)=	Nederland 180 %	België 121 %
1 x per week	27	16
1 x per maand	12	11
Elke 6 maanden	2	5
Elke 12 maanden	3	3
Alleen wanneer er een bedreiging is aangekondigd	2	3
Gaat volledig automatisch	51	50
Nooit	1	6
Wn/ga	4	8

Frequentie downloaden patches

De frequentie van het downloaden van patches ligt op een vergelijkbaar niveau als van de updates. Echter, dit gebeurt in mindere mate automatisch. Opvallend is dat circa één op de vijf bedrijven in België aangeeft dat dit nooit gebeurt. Bovendien geeft een kwart van de ondervraagden aan het niet te weten.

Hoe vaak worden <u>patches</u> gedownload? Basis (100%)=	Nederland 180 %	België 121 %
1 x per week	19	9
1 x per maand	13	8
Elke 6 maanden	7	6
Elke 12 maanden	4	2
Alleen wanneer er een bedreiging is aangekondigd	6	4
Gaat volledig automatisch	39	28
Nooit	4	19
Wn/ga	8	25



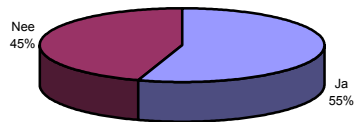
Maatregelen tegen 'interne' bedreigingen

Aan alle bedrijven is (geholpen) gevraagd welke maatregelen men heeft genomen tegen 'interne' bedreigingen. Circa eenderde van alle bedrijven heeft een beleid opgesteld op het gebied van beveiliging. Eén op de vier bedrijven traint haar medewerkers op dit gebied. Verreweg de meeste bedrijven gebruiken een password op elke PC. Opvallend is dat circa 10% in Nederland en ongeveer 20% van de bedrijven in België geen maatregelen heeft getroffen.

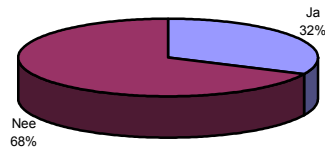
Welke van de volgende maatregelen neemt u tegen 'interne' bedreigingen? Basis (100%)=	Nederland 180 %	België 121 %
Password op elke PC/Laptop	81	78
Beveiliging remote users	28	35
Beveiligingssoftware op mobiele devices	15	17
Security policy	36	32
Bewustwording/trainingen van alle medewerkers	28	24
Webfilters voor afschermen van bepaalde sites	26	17
Anders	4	-
Geen	11	21

Iets minder dan de helft van de Nederlandse bedrijven heeft geen extra beveiligingsmaatregelen genomen voor vertrouwelijke informatie. In België is dit ruim tweederde.

Nederland



België



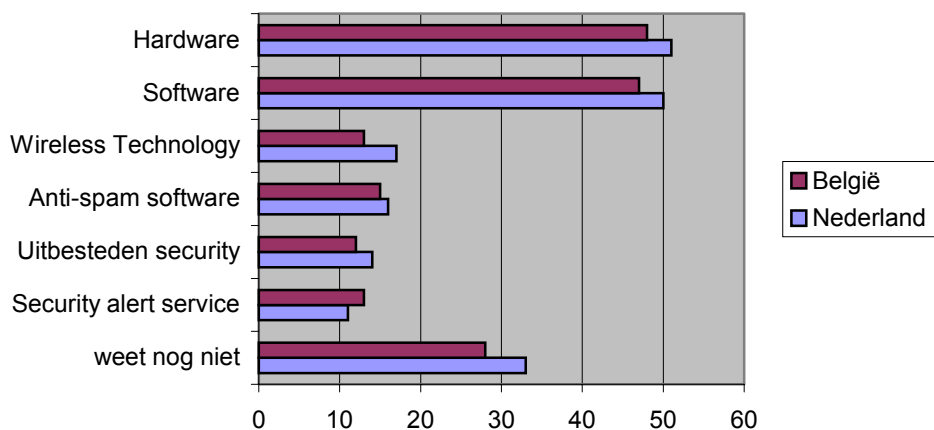
3.2 De toekomst

Aan alle bedrijven is gevraagd of men verwacht dat het bedrijf de komende 6 maanden zal uitbreiden of juist zal verminderen wat betreft personeel, totale ICT-budget en budget voor IT-beveiliging. Het merendeel van de bedrijven geeft aan dat de budgetten hetzelfde zullen blijven. Dit geldt voor zowel het totale ICT budget als voor het IT-beveiligingsbudget. Circa één op de zeven bedrijven geeft aan een toename te verwachten.

De volgende vragen over de toekomstplannen van uw bedrijf. Kunt u van de volgende zaken aangeven of u verwacht dat uw bedrijf de komende 6 maanden zal uitbreiden of juist zal verminderen? Basis (100%)=	Nederland 180 %	België 121 %
<u>Personeel</u>		
Meer	22	27
Blijft hetzelfde	69	64
Minder	7	9
Wn/ga	2	1
<u>Totale ICT-budget</u>		
Meer	16	13
Blijft hetzelfde	66	67
Minder	9	2
Wn/ga	10	18
<u>Budget voor IT-beveiliging</u>		
Meer	15	14
Blijft hetzelfde	70	61
Minder	6	2
Wn/ga	9	24

Interesse in producten

Circa de helft van alle bedrijven verwacht de komende 6 maanden software en hardware aan te schaffen. Dit zijn in Nederland vooral de grote bedrijven van 50-250 werknemers. In België zijn de kleinere bedrijven (5-9 werknemers) relatief meer geïnteresseerd in security alert service en anti-spam software dan de overige bedrijven.



3.3 Informatie en verkoopkanalen

Bronnen van informatie

Veel Nederlandse bedrijven informeren zich over IT-beveiliging via internet en via de vakbladen. Internet krijgt als informatiebron de voorkeur. De softwareleverancier speelt daarnaast ook een belangrijke rol. Circa één op de vijf bedrijven geeft de voorkeur aan het ontvangen van informatie via hun softwareleverancier. Een opvallend verschil met België, is dat in Nederland de security consultants relatief vaker een rol spelen in het informatieproces. Verder wordt in België minder vaak internet geraadpleegd als informatiebron. De voorkeur gaat echter wel uit naar dit medium. Ook in België spelen de softwareleveranciers en de IT-bladen een prominente rol.

Via welke media of bronnen laat u zich informeren over IT-beveiliging? Basis (100%)=	Nederland Gebruikt wel eens 180 %	Gebruikt meestal 159 %	Voorkeur voor 180 %
Abonn. virus alert service	4	2	2
Abonn. security alert service	-	-	-
Vendors van security solutions	1	-	-
Security consultants	14	11	9
Mijn softwareleverancier	36	23	19
Familie/vrienden	3	1	1
Zakelijke contacten (niet IT)	6	4	3
Internet	39	31	38
IT-bladen	30	13	13
Radio/TV	1	-	1
Via externe partij	2	1	1
Via collega/medewerker	4	2	-
Via folders	4	1	4
E-mail/nieuwsgroepen	1	1	3
Anders	2	3	
Geen	8		13

Via welke media of bronnen laat u zich informeren over IT-beveiliging? Basis (100%)=	België Gebruikt wel eens 121 %	Gebruikt meestal 95 %	Voorkeur voor 121 %
Abonn. virus alert service	3	3	1
Abonn. security alert service	2	2	2
Vendors van security solutions	1	1	-
Security consultants	4	3	2
Mijn softwareleverancier	25	25	20
Familie/vrienden	5	1	1
Zakelijke contacten (niet IT)	7	-	1
Internet	19	19	34
IT-bladen	24	12	16
Radio/TV	4	-	2
Via externe partij	13	4	9
Via collega/medewerker	2	5	1
Via folders	3	3	-
E-mail/nieuwsgroepen	1	-	4
Anders	8	4	
Geen	18		22



Verkoopkanalen

De distributiekkanalen waar men de software koopt zijn divers. Het wordt veelal direct bij een winkel gekocht of via een tussenpartij zoals een consultant. Er wordt relatief weinig direct afgenomen bij de softwareleverancier zelf.

Waar of hoe koopt u bij voorkeur uw software? Basis (100%)=	Nederland 180 %	België 121 %
Kleine plaatselijke dealer	21	31
Mailorder	4	2
Online /web	12	8
Consultant	24	23
Retail winkel (bijv. Vobis)	13	5
B-to-B winkel (bijv. Office Center)	20	15
Kantoorvakhandel	3	1
Via externe partij	2	12
Direct bij softwareleverancier/distributeur	6	8

Hoeveel werknemers (inclusief uzelf) zijn er binnen uw bedrijf werkzaam? Basis (100%)=	Nederland 180 %	België 121 %
5-9 werknemers	43	44
10-19 werknemers	26	27
20-49 werknemers	18	19
50-250 werknemers	13	10

Wordt er binnen uw bedrijf gebruik gemaakt van internet en/of e-mail? Basis (100%)=	Nederland 180 %	België 121 %
Ja	100	100
Nee	-	-

Bent u (mede) verantwoordelijk voor ICT (software/hardware) en internetbeveiliging? Basis (100%)=	Nederland 180 %	België 121 %
Ja	100	100
Nee	-	-

Hoe is de ICT/internet beveiliging binnen uw bedrijf georganiseerd? Is dat ... Basis (100%)=	Nederland 180 %	België 121 %
Een werknemer doet het erbij	42	51
Er is een ICT afdeling	14	3
Er is één ICT persoon	22	33
Een externe partij (wordt geheel/gedeeltelijk uitbesteed)	34	41
anders	2	2

Welke van de volgende oplossingen worden gebruikt om uw bedrijfsdata te beveiligen? Basis (100%)=	Nederland 180 %	België 121 %
Antivirus software	95	92
Firewalls	72	56
Intrusion detection	18	17
Content filtering	20	11
VPN	23	11
Wn/ga	1	6

Welke onderdelen van het netwerk worden beveiligd? Basis (100%)=	Nederland 180 %	België 121 %
Desktops	76	78
Servers	78	64
Gateway	47	38
Mobiele services	16	17
Laptops/remote users	42	54

Hoe vaak wordt de software bijgewerkt? Basis (100%)=	Nederland 180 %	België 121 %
1 x per week	27	16
1 x per maand	12	11
Elke 6 maanden	2	5
Elke 12 maanden	3	3
Alleen wanneer er een bedreiging is aangekondigd	2	3
Gaat volledig automatisch	51	50
Nooit	1	6
Wn/ga	4	8

Hoe vaak worden patches gedownload? Basis (100%)=	Nederland 180 %	België 121 %
1 x per week	19	9
1 x per maand	13	8
Elke 6 maanden	7	6
Elke 12 maanden	4	2
Alleen wanneer er een bedreiging is aangekondigd	6	4
Gaat volledig automatisch	39	28
Nooit	4	19
Wn/ga	8	25

Welke van de volgende maatregelen neemt u tegen 'interne' bedreigingen? Basis (100%)=	Nederland 180 %	België 121 %
Password op elke PC/Laptop	81	78
Beveiliging remote users	28	35
Beveiligingssoftware op mobiele devices	15	17
Security policy	36	32
Bewustwording/trainingen van alle medewerkers	28	24
Webfilters voor afschermen van bepaalde sites	26	17
Anders	4	-
Geen	11	21

Heeft u het idee dat uw bedrijfsnetwerk <u>voldoende</u> beveiligd is? Basis (100%)=	Nederland 180 %	België 121 %
Ja	86	75
Nee	13	25

Heeft u extra beveiligingsmaatregelen voor vertrouwelijke informatie? Basis (100%)=	Nederland 180 %	België 121 %
Ja	55	32
Nee	45	68

Waarvoor gebruikt u internet bij de bedrijfsvoering? Is dat .. Basis (100%)=	Nederland 180 %	België 121 %
E-mail	96	96
Website alleen voor informatie	78	79
Website informatie en e-business	47	40

Via welke media of bronnen laat u zich informeren over IT-beveiliging? Basis (100%)=	Nederland 180 %	België 121 %
Abonn. virus alert service	4	3
Abonn. security alert service	-	2
Vendors van security solutions	1	1
Security consultants	14	4
Mijn softwareleverancier	36	25
Familie/vrienden	3	5
Zakelijke contacten (niet IT)	6	7
Internet	39	19
IT-bladen	30	24
Radio/TV	1	4
Via externe partij	2	13
Via collega/medewerker	4	2
Via folders	4	3
E-mail/nieuwsgroepen	1	1
Anders	2	8
Geen	8	18

Welk medium of bron gebruikt u het <u>meest</u> ? Basis (100%)=	Nederland 159 %	België 95 %
Abonn. virus alert service	2	3
Abonn. security alert service	-	2
Vendors van security solutions	-	1
Security consultants	11	3
Mijn softwareleverancier	23	25
Familie/vrienden	1	1
Zakelijke contacten (niet IT)	4	-
Internet	31	19
IT-bladen	13	12
Radio/TV	-	-
Via externe partij	1	4
Via collega/medewerker	2	5
Via folders	1	3
E-mail/nieuwsgroepen	1	-
Anders	3	4

Hoe zou u bij voorkeur geïnformeerd willen worden over IT-beveiliging? Basis (100%)=	Nederland 180 %	België 121 %
Abonn. virus alert service	2	1
Abonn. security alert service	-	2
Vendors van security solutions	-	-
Security consultants	9	2
Mijn softwareleverancier	19	20
Familie/vrienden	1	1
Zakelijke contacten (niet IT)	3	1
Internet	38	34
IT-bladen	13	16
Radio/TV	1	2
Via externe partij	1	9
Via collega/medewerker	-	1
Via folders	4	-
E-mail/nieuwsgroepen	3	4
Geen voorkeur	13	22

De volgende vragen over de toekomstplannen van uw bedrijf. Kunt u van de volgende zaken aangeven of u verwacht dat uw bedrijf de komende 6 maanden zal uitbreiden of juist zal verminderen? Basis (100%)=	Nederland 180 %	België 121 %
<u>Personeel</u>		
Meer	22	27
Blijft hetzelfde	69	64
Minder	7	9
Wn/ga	2	1
<u>Totale ICT-budget</u>		
Meer	16	13
Blijft hetzelfde	66	67
Minder	9	2
Wn/ga	10	18
<u>Budget voor IT beveiliging</u>		
Meer	15	14
Blijft hetzelfde	70	61
Minder	6	2
Wn/ga	9	24

Kunt u aangeven of u verwacht dat uw bedrijf de komende 6 maanden één van de volgende zaken zal aanschaffen? Basis (100%)=	Nederland 180 %	België 121 %
Software	50	47
Hardware	51	48
Wireless Technology	17	13
Security alert service	11	13
Anti-spam software	16	15
Uitbesteden security	14	12
Wn/ga	33	28

Kunt u aangeven welk percentage van het totale budget van uw bedrijf wordt gereserveerd voor ICT? Basis (100%)=	Nederland 180 %	België 121 %
0%	1	2
1%	9	11
2-5%	22	21
6-10 %	10	7
11-20%	6	7
25-50%	3	5
> 50%	2	1
Gemiddeld	10	8
Std. Dev.	16.1	10.8

Is er binnen uw bedrijf een apart budget gereserveerd voor internet beveiliging? Basis (100%)=	Nederland 180 %	België 121 %
Ja	10	9
Nee	83	89
Wn/ga	7	2

Kunt u aangeven welk percentage van het totale ICT budget van uw bedrijf wordt gereserveerd voor internetbeveiliging? Basis (100%)=	Nederland 18 %	België 11 %
0		17
1%	11	7
2-5%	22	7
6-10 %	6	13
11-20%	6	-
25-50%	11	-
> 50%	-	-
Wn/ga	39	56
Gemiddeld	10	4
Std. Dev.	10.4	5

Waar of hoe koopt u bij voorkeur uw software? Basis (100%)=	Nederland 180 %	België 121 %
Kleine plaatselijke dealer	21	31
Mailorder	4	2
Online /web	12	8
Consultant	24	23
Retail winkel (bijv. Vobis)	13	5
B-to-B winkel (bijv. Office Center)	20	15
Kantoorvakhandel	3	1
Via externe partij	2	12
Direct bij softwareleverancier/distributeur	6	8

Als incentive tijdens het bellen kunnen we melden dat de deelnemers kans maken op een firewall/vpn appliance of een reischeque twv 500 euro.
Uiteraard alleen indien zij aan het gestelde profiel voldoen, helpt misschien om ze over de streep te trekken.

Bijlage: Vraagpuntenlijst

Goede, u spreekt met Van Morph Research, een onderzoekburo uit Den Haag. Momenteel voeren wij een onderzoek uit naar internetbeveiliging binnen het Midden en Klein bedrijf. Het vraaggesprek duurt een minuut of zeven. Deelnemers aan het onderzoek maken kans op een reischeque twv 500 euro of een internetbeveiliging applicatie.

Om te bepalen of u in de steekproef valt heb ik een drietal vraagjes:

Selectievragen:

Hoeveel werknemers (inclusief u zelf) zijn er binnen uw bedrijf werkzaam?

1-4 = EINDE = NIEUW CONTACT

5-9

10-19

20-49

50-250

251 of meer = EINDE = NIEUW CONTACT

Wordt er binnen uw bedrijf gebruik gemaakt van internet en/of e-mail?

Ja

Nee = EINDE= NIEUW CONTACT

Bent u (mede) verantwoordelijk voor ICT (software/hardware) en internet beveiliging?

Ja

Nee

Indien Nee, zou ik kunnen spreken met de persoon die hierover gaat?

(INT: leg aan deze nieuwe persoon uit waar over het gaat)

Start vragenlijst:

Hoe is de ICT/internet beveiliging binnen uw bedrijf georganiseerd?

(INT: antwoorden voorlezen; slechts 1 antwoord mogelijk)

- Een werknemer doet het 'erbij'
- Er is een ICT-afdeling
- Er is één ICT-persoon
- Een externe partij (wordt geheel/gedeeltelijk uitbesteed)
- Anders, nl....

Welke van de volgende oplossingen worden gebruikt om uw bedrijfsdata te beveiligen?

(INT: antwoorden voorlezen; meerdere antwoorden mogelijk)

- Antivirus software (beschermt tegen virussen, spoort virussen op en houdt ze tegen)
- Firewalls (beschermt tegen hackers, voorkomt ongeautoriseerde toegang tot het bedrijfsnetwerk of de standalone pc)
- Intrusion detection (inbraakdetectie, verbetert de firewall beveiliging door mogelijk schadelijk internetverkeer te herkennen en automatisch alle communicatie met de indringer te beëindigen)
- Content filtering (filtering op basis van de inhoud van e-mailberichten, webpagina's)
- VPN (virtual private network, een veilig netwerk uitgevoerd in een openbaar netwerk; bijv voor veilige communicatie tussen twee instellingen via het internet)
- Geen van allen

Welke onderdelen van het netwerk worden beveiligd?

(meerdere antwoorden mogelijk)

(INT: Antwoorden in wisselende volgorde voorlezen)

- Desktops
- Servers
- Gateway (verbinding tussen bedrijfsnetwerk en de buitenwereld, functioneert als toegangspoort tot het netwerk)
- Mobiele devices (handhelds, pda's)
- Laptops – Remote users (gebruikers op afstand, krijgen via remote access toegang tot het bedrijfsnetwerk)

Hoe vaak wordt de software bijgewerkt?

(slechts 1 antwoord mogelijk)

- 1 x per week
- 1 x per maand
- Elke 6 maanden
- Elke 12 maanden
- Alleen wanneer er een bedreiging is aangekondigd
- Dit gaat volledig automatisch
- Nooit
- Weet niet

Hoe vaak worden patches gedownload?

(slechts 1 antwoord mogelijk)

(patches: reparatiesoftware; kleine wijzigingen die direct in een programma worden doorgevoerd om het desbetreffende programma te repareren of te verbeteren)

- 1 x per week
- 1 x per maand
- Elke 6 maanden
- Elke 12 maanden
- Alleen wanneer er een bedreiging is aangekondigd
- Dit gaat volledig automatisch
- Nooit
- Weet niet

Welke van de volgende maatregelen neemt u tegen 'interne' bedreigingen?

(meerdere antwoorden mogelijk)

(interne bedreigingen: bedreigingen die binnen het bedrijfsnetwerk ontstaan doordat werknemers handelingen verrichten die het netwerk in gevaar brengen. Bijv. het downloaden van programma's, openen van onbekende e-mail bijlagen, wachtwoorden en virusbescherming niet tijdig bijwerken etc)

- Passwords op elke PC/Laptop
- Beveiligen remote users
- Beveiligingssoftware op mobiele devices, bv PDA's
- Security policy *(beleid, procedure, regels e.d. op het gebied van beveiliging)*

- Bewustwording/training van alle medewerkers
- Webfilters voor afschermen van bepaalde sites
- Overig, nl.:
- Geen

Heeft u het idee dat uw bedrijfsnetwerk voldoende beveiligd is?

- Ja
- Nee

Heeft u extra beveiligingsmaatregelen voor vertrouwelijke informatie?

- Ja
- Nee

Waarvoor gebruikt u internet bij de bedrijfsvoering?

(meerdere antwoorden mogelijk)

- E-mail
- Website – alleen voor informatie
- Website – informatie en e-business

Via welke media of bronnen laat u zich informeren over IT-beveiliging?

(meerdere antwoorden mogelijk)

INT: niet helpen)

Welk medium of bron gebruikt u het meest?

(INT: evt de genoemde bronnen voorlezen waaruit men moet kiezen)

slechts één antwoord mogelijk)

- Abonnement virus alert service (viralert.nl, waarschuwingdienst.nl)
- Abonnement security alert service (microsoft, sun, security focus Vendors van security solutions (bvb Cisco, Symantec)
- Security consultants
- Mijn softwareleverancier
- Familie of vrienden
- Zakelijke contacten, niet IT-gerelateerd
- Internet
- IT-bladen
- Radio/TV
- Overig, nl.:
- Geen

Hoe zou u bij voorkeur geïnformeerd willen worden over IT-beveiliging (mogelijke bedreigingen e.d.)?

(INT: niet voorlezen; meerdere antwoorden mogelijk)

- Abonnement virus alert service
- Abonnement security alert service
- Vendors van security solutions
- Security consultants
- Familie of vrienden
- Zakelijke contacten, niet IT-gerelateerd
- Internet
- IT-bladen
- Radio/TV
- Anders, nl.:
- Geen voorkeur

De volgende vragen gaan over de toekomstplannen van uw bedrijf.

Kunt u van de volgende zaken aangeven of u verwacht dat uw bedrijf de komende 6 maanden zal uitbreiden of juist zal minderen:

- Personeel
- Totale ICT budget
- Budget voor IT-beveiliging

(meer, blijft hetzelfde, minder)

Kunt u aangeven of u verwacht u dat uw bedrijf de komende 6 maanden een van de volgende zaken zal aanschaffen:

(INT: antwoorden voorlezen)

- Software
- Hardware
- Wireless technology (*draadloze technologie, die wordt gebruikt voor draadloze netwerken*)
- Security alert service (*dienst die waarschuwingen geeft voor bedreigingen op internet zoals virussen, hacking, kwetsbaarheden. Informeert ook wanneer bepaalde 'patches' beschikbaar zijn*)
- Anti-spam software
- Uitbesteden security
- Anders, nl.

Kunt u aangeven welk percentage van het totale budget van uw bedrijf wordt gereserveerd voor ICT?

.. %

Is er binnen uw bedrijf een apart budget gereserveerd voor Internet beveiliging?

- Ja
- Nee

Kunt u aangeven welk percentage van het totale ICT budget van uw bedrijf wordt gereserveerd voor Internet beveiliging?

Waar of hoe koopt u bij voorkeur uw software?

(INT: meerdere antwoorden mogelijk)

Bijvoorbeeld:

- Kleine plaatselijke dealer
- Mailorder (via postorder, bvb Inmac, 06 software)
- Online/web
- Consultant
- Retail winkel (bvb Vobis, Dynabyte)
- B-to-b winkel (Office Centre, Makro)
- Kantoorvakhandel
- Anders, nl:

Kunt u tenslotte aangeven in welke branche u bedrijf hoofdzakelijk actief is?
(slechts één antwoord mogelijk)

Banken en Financiële instellingen
Bouw, architecten, aannemers en makelaars
Chemische- en farmaceutische industrie
Distributie en handel
Electronische en geprinte media
Gezondheidszorg
Groothandel en retail
Horeca
Industriële onderneming
IT industrie
Non-profit
Onderwijs
Openbare instellingen
Overheid
Productie/distributie van olie, electriciteit en gas
Staal- en metaalindustrie
Telecom
Textiel
Transportindustrie
Voedingsmiddelenindustrie
Zakelijke dienstverlening
Anders, nl.

Dit was de laatste vraag. Wij danken u vriendelijk voor uw medewerking en wensen u nog een prettige dag.