



Internet Veiligheidspakket

Dienstbeschrijving

Inhoudsopgave

1	Gebruikte definities en afkortingen.....	3
2	Internet Veiligheidspakket	5
2.1	Beschrijving van de dienst	5
2.2	Internet Veiligheidspakket partner F-Secure	5
2.3	Internet Veiligheidspakket functionaliteiten	6
2.3.1	<i>Virus- en spywarebeveiliging</i>	6
2.3.2	<i>Internet Shield</i>	6
2.3.3	<i>URL filtering/blocking</i>	6
2.3.4	<i>Spambeveiliging</i>	6
2.3.5	<i>Server beveiliging</i>	7
2.3.6	<i>Mobiele beveiliging</i>	7
2.3.7	<i>Beheerportaal</i>	7
2.3.8	<i>Automatische updates</i>	7
2.3.9	<i>Overzicht van de pakketten bij het Internet Veiligheidspakket</i>	8
2.4	Waarom hebt u het Internet Veiligheidspakket nodig?	8
3	Voordelen van Internet Veiligheidspakket	9
3.1	Ondersteunde besturingssystemen	9
3.1.1	<i>Systeemeisen</i>	9
4	Service Level Agreements.....	12
4.1	Openstellingtijden Business Servicedesk	12
4.2	Beschikbaarheid	12
4.3	Maintenance Window	12
5	Helpdesk ingang en procedure.....	13
5.1	Openstellingtijden Business Servicedesk	13
5.2	Communicatie omtrent onderhoud.....	13
5.3	Escalaties	13
6	Facturatie	14
6.1	Tariefstructuur.....	14
6.2	Facturering	14
6.3	Contractsduur	14
7	Informatiebeveiliging	13
7.1	De ISO 27001 en ISO 27002 richtlijn hoe te implementeren.....	143
7.2	Continuïteitsbeheer.....	13
7.3	Beveiligingsmaatregelen.....	143

1 Gebruikte definities en afkortingen

Aan de met een hoofdletter geschreven begrippen komt de volgende betekenis toe:

Term	Definitie
Internet Veiligheidspakket	Klantbeveiligingssoftware
Serviceprovider	Entiteit die de dienst Internet Veiligheidspakket bij de eindgebruiker brengt. KPN wordt hierbij aangemeten als een service provider.
Update	Een updatepakket of -bestand, dat wordt gebruikt voor het bijwerken van databases of van configuratiegegevens zoals gebruikt door de softwareapplicatie.
Upgrade	Een kleine softwarerelease, onderhouds upgrade, servicerelease, servicepack of fix voor de softwareapplicatie, en/of ii) een nieuwe grote release van de softwareapplicatie.
Service Provider	KPN als Application Service Provider
MKB-klant	Een kleine of middelgrote zakelijke klant
Eindgebruiker	Een werknemer van een MKB-klant die de klantbeveiligingssoftware gebruikt



2 Internet Veiligheidspakket

Deze dienstbeschrijving maakt samen met de Algemene Voorwaarden Software Online en aanvullende F-Secure licentie voorwaarden onderdeel uit van alle Overeenkomsten tot het leveren van het Internet Veiligheidspakket, vanaf 1 mei 2008. Bij het verschijnen van een nieuwere versie (KPN behoudt zich hiertoe het recht voor) zal deze versie geldig blijven voor alle lopende overeenkomsten op basis van deze versie.

2.1 Beschrijving van de dienst

Modern zakendoen is sterk afhankelijk van computers. Toch beschikken veel kleine en middelgrote bedrijven nog steeds niet over een up-to-date beveiligingsoplossing die hun bedrijfsmiddelen beschermt. Het meest ernstige gevolg hiervan kan zijn dat er vanwege malware-aanvallen van hackers en indringers waardevolle data verloren gaat. Als een bedrijf een vrijplaats voor spammers wordt, kan dit leiden tot diefstal van data, verlies van omzet en kan er zelfs ernstige schade aan de reputatie van een bedrijf toegebracht worden.

Slimme bedrijven kiezen voor beveiliging in de vorm van een abonnement. In een tijd van beperkte middelen en budgetten voor IT-beveiliging, een steeds mobieler wordende kantooromgeving en steeds meer doelgerichte aanvallen is een abonnement de beste keus die u kunt maken.

Bedrijven kunnen zich volledig richten op zakendoen, zonder zich zorgen te maken over licenties, updates of interne IT-beveiliging. Dat wordt allemaal aan de experts overgelaten.

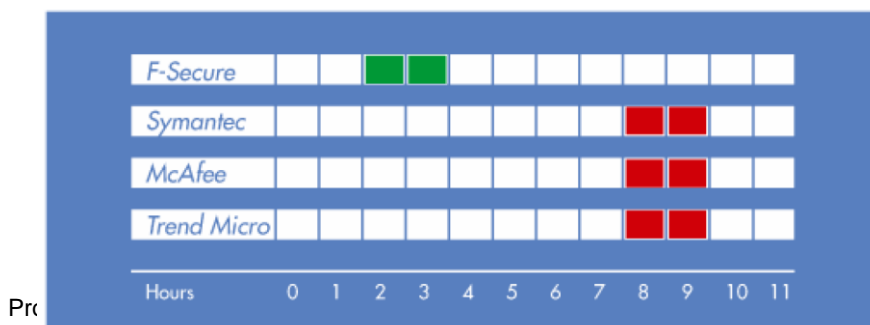
Met het Internet Veiligheidspakket biedt KPN u een nieuwe en gemakkelijke manier om uzelf ervan te verzekeren dat uw bedrijf optimaal beschermd is tegen bedreigingen: een complete oplossing bestaande uit beveiligingssoftware en een beheerportaal.

Het Internet Veiligheidspakket bestaat uit virus- en spyware beveiliging, Internet Shield, rootkit-detector en een url filterings functionaliteit om volledige bescherming te garanderen – zelfs buiten de firewall van het bedrijf. De ingebouwde spam detectie zorgt ervoor dat uw e-mail gevrijwaard blijft van junkmail en andere ongewenste berichten.

2.2 Internet Veiligheidspakket partner F-Secure

F-Secure heeft een bewezen staat van dienst als het gaat om snel reageren op nieuwe bedreigingen. We zijn de markt telkens een stap voor in het ontwikkelen van bescherming tegen nieuwe schadelijke software (malware). Snelheid is belangrijk – hoe sneller u beschermd bent, des te kleiner de kans dat u tegen problemen oploopt. Er verschijnen voortdurend nieuwe bedreigingen die zich razendsnel verspreiden, of u dat nu leuk vindt of niet.

Versie 1.1



2.3 Internet Veiligheidspakket functionaliteiten

Het Internet Veiligheidspakket is door F-Secure en KPN ontwikkeld en bevat een volledig geïntegreerde bescherming tegen virussen en spyware, een persoonlijke firewall, URL filtering, pop-upblokkering en spamfilter, waarmee u uzelf eenvoudig in één keer kunt beschermen tegen internetbedreigingen. Het Internet Veiligheidspakket omvat de volgende functionaliteiten:

2.3.1 Virus- en spywarebeveiliging

Virus- en spywarebeveiliging detecteert en blokkeert schadelijke software (malware) die uw computer kan aanvallen via e-mail, via verwisselbare media, of wanneer u materiaal van internet download. Het beschermt uw privacy door heimelijk geïnstalleerde gegevensverzamelende software van uw computer te verwijderen. Virus- en spyware beveiliging:

- plaatst reeds op uw computer geïnstalleerde schadelijke software 'in quarantaine' en verwijdert deze;
- blokkeert opdringerige reclame-popups;
- beschermt uw systeeminstellingen; en detecteert potentieel schadelijke software (riskware) en plaatst deze in quarantaine of verwijdert deze.

Het antivirus-onderzoekscentrum publiceert en ververscht dagelijks de virusdefinities. Gebruikers ontvangen automatisch de nieuwste virusdefinities en updates van de spyware-database.

2.3.2 Internet Shield


Internet Shield beschermt uw computer tegen ongeautoriseerde pogingen om een verbinding tot stand te brengen, interne aanvallen, informatiediefstal, kwaadaardige applicaties en andere ongewenste applicaties, zoals peer-to-peer-software. De firewall is een belangrijk onderdeel van Internet Shield. Wanneer Internet Shield op uw computer geïnstalleerd is, beschikt u over firewallbescherming, zelfs wanneer u niet op het lokale bedrijfsnetwerk bent aangesloten. Wanneer een internetverbinding geactiveerd is, wordt de firewall-software automatisch bijgewerkt.

2.3.3 URL filtering/blocking

Hiermee kunt u toezicht uitoefenen om (uw) medewerkers te beschermen tegen ongeschikte informatie op het internet - zoals geweld, drugs en sex. U kunt instellen hoeveel vrijheid medewerkers hebben bij het gebruik van internet op de computer. Zo vermijdt u dat medewerkers op sites terechtkomen die niet voor hen bestemd zijn. Met deze vorm van toezicht bepaalt u tevens het wachtwoord waarmee u de instellingen van het Internet Veiligheidspakket kunt wijzigen, en waarmee u toezicht op uw medewerkers beheert.

N.B.: Met het beheerportaal kunt u alle apparaten die voorzien zijn van het Internet Veiligheidspakket op afstand beheren en voorzien van bedrijfspolicy's.

2.3.4 Spambeveiliging



De spambeveiligingsfunctie bewaakt inkomende e-mail en verwijdert ongevraagde e-mails (spam) uit uw postvak. Zodra een e-mail als spam wordt herkend, wordt deze als zondanig aangemerkt en in een afzonderlijke map geplaatst.

2.3.5 Server beveiliging

Naast de beveiliging van het werkstation is de beveiliging van servers ook opgenomen in de dienstverlening. De servers worden net zoals werkstations beveiligd tegen de bedreigingen van het internet. De server beveiliging bestaat uit virus & spywarebescherming.

Server beveiliging wordt meegeleverd als onderdeel van de pakketten vanaf 5 medewerkers.

2.3.6 Mobiele beveiliging

Mobiele apparatuur met geavanceerde mogelijkheden waaronder internet en e-mail worden met toenemende mate standaard binnen veel bedrijven. Deze apparaten zijn niet alleen veelvuldig verbonden met het internet, ze staan onderling ook veel met elkaar in verbinding met bijvoorbeeld Bluetooth. Daarmee zijn mobiele apparaten net zo kwetsbaar voor hackers, spyware en virussen als een normale PC. KPN verwacht dan ook dat deze kwetsbare apparatuur in toenemende mate het slachtoffer wordt van diverse vormen van malware.

Om deze reden heeft KPN de beveiliging van mobiele apparatuur opgenomen in haar dienstverlening. De mobiele beveiliging is software die u op uw mobiele apparaat installeert en uw apparaat automatisch beschermt tegen bedreigingen. Ook de software op uw mobiele apparaat wordt automatisch voorzien van de nieuwste updates. De mobiele beveiliging bestaat uit anti-virus software en een firewall.

Mobiele beveiliging wordt meegeleverd als onderdeel van de pakketten vanaf 5 medewerkers en zal medio september 2008 meegeleverd worden bij deze pakketten.

2.3.7 Beheerportaal

Het beheerportaal is een website die u in staat stelt om uw licentiecodes te beheren. Alle door u aangevraagde licenties worden automatisch opgenomen in deze beheerportaal waarin u kunt zien wat de huidige status van uw licenties is. Hierin kunt u bijvoorbeeld zien of bepaalde installaties al uitgevoerd zijn, of de software van de laatste updates is voorzien, of alle programma onderdelen aanstaan en welk profiel toegepast is. Daarnaast kunt u vanuit het beheerportaal de profielen op de lokale installaties toepassen.

Het beheerportaal wordt meegeleverd als onderdeel van de pakketten vanaf 5 medewerkers.

2.3.8 Automatische updates

F-Secure verzorgt voor KPN de hosting van de updatedienst van de klantbeveiligingssoftware en onderhoudt deze. Wanneer eindgebruikers van de klantbeveiligingssoftware verbinding maken met het internet, controleert de update-dienst op mogelijke wijzigingen van de productconfiguratie, de beschikbare software-, beveiligings- en profielupdates, en de beveiligingsprofielen en -upgrades. Eindgebruikers met een geldig abonnement ontvangen de updates, upgrades en nieuwe beveiligingsprofielen automatisch.

2.3.9 Overzicht van de pakketten bij het Internet Veiligheidspakket

Internet Veiligheidspakket*	1	2	3	4	5	6	7	8	9
Aantal apparaten**	2	5	10	20	30	40	50	75	100
PC beveiliging	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Server beveiliging	Nee	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Mobiele beveiliging***	Nee	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Beheerportaal	Nee	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja

* U kunt een abonnement alleen upgraden naar een groter pakket, downgraden is niet mogelijk

** Aantal PC's, Servers of Mobiele devices die beveiligd kunnen worden

*** Deze optie is pas gereed medio september 2008

Internet Veiligheidspakket	Virus & Spywarebescherming	Internet Shield	URL filtering	Spam beveiliging	Firewall
PC beveiliging	Ja	Ja	Ja	Ja	Ja
Server beveiliging	Ja	n.v.t.	n.v.t.	n.v.t.	n.v.t.
Mobiele beveiliging*	Ja	n.v.t.	n.v.t.	n.v.t.	Ja

* Deze optie is pas gereed medio september 2008

2.4 Waarom hebt u het Internet Veiligheidspakket nodig?

- 80% van de klein zakelijke computergebruikers is besmet met spyware/adware
- 67% van de eindgebruikers heeft geen actuele antivirussoftware
- 82% van alle binnenkomende berichten is spam
- Er worden elke dag zo'n 10 tot 15 nieuwe virussen ontdekt
- Er bestaan op dit moment meer dan 185.000 virussen

3 Voordelen van Internet Veiligheidspakket

De voordelen van het Internet Veiligheidspakket zijn duidelijk. Uw beveiliging wordt kundig en efficiënt verzorgd door deskundigen, zodat u zich volledig op uw bedrijf kunt richten.

- Voordelige abonnementsprijzen: u betaalt slechts een maandelijks bedrag voor het aantal licenties dat u nodig heeft.
- Aan te passen aan uw zakelijke behoeften dankzij handige product- en licentiecombinaties.
- Eenvoudig installatiebeheer en flexibel gebruik van licenties (direct overzicht van de licentie- en installatiestatus) door middel van het Beheerportaal.
- Eenvoudig te installeren via de webpagina van KPN.com of met behulp van een cd.
- Complete beveiligingsoplossing inclusief virus- en spywarebeveiliging, Internet Shield, spamdetectie en url filtering.
- Minimale onderhoudsinspanningen vereist – de automatische virusdefinitie-updates en software-upgrades worden direct aan uw computer geleverd.
- Vooraf opgestelde beveiligingsprofielen voor verschillende gebruikersgroepen met uiteenlopende behoeftes.
- Bescherming van uw kwetsbare mobiele apparatuur
- Ondersteuning vanuit KPN bij problemen

3.1 Ondersteunde besturingssystemen

Het Internet Veiligheidspakket ondersteunt de onderstaande besturingssystemen:

- Windows 98, Windows 98SE, Windows ME
- Windows 2000 Professional SP4
- Windows XP Professional of Home Edition SP2
- Windows Vista (32-bit)
- Windows Server 2000 & 2003

3.1.1 Systeemeisen

Uw computer moet aan de volgende eisen voldoen om de klantbeveiligingssoftware van F-Secure Protection Service for Business te kunnen installeren en uitvoeren:

Internet Veiligheidspakket voor werkplekken:

- Besturingssysteem: Windows 2000-SP4 / XP / Vista 32-bit
- Processor: Intel Pentium III 600Mhz of hoger
- Geheugen: Windows 2000/XP 256 MB, Windows Vista 512 MB
- Schijfruimte: 500MB vrije schijfruimte (300 MB voor alleen Anti-virus)
- Beeldscherm: Min. 8-bit (256 kleuren)

- Internet verbinding: Een Internet verbinding is noodzakelijk om de laatste virusinformatie en updates te ontvangen.
- Browser: Internet Explorer 6.0 of hoger.

Internet Veiligheidspakket voor Servers:

- Besturingssysteem: Microsoft Windows 2000 Server, Windows Server 2003
- Processor: Intel Pentium III 800Mhz of hoger
- Geheugen: 512 MB
- Schijfruimte: 300MB vrije schijfruimte
- Beeldscherm: Min. 8-bit (256 kleuren)
- Internet verbinding: Een Internet verbinding is noodzakelijk om de laatste virusinformatie en updates te ontvangen.
- Browser: Internet Explorer 6.0 of hoger.

N.B.: De minimale vereisten hebben betrekking op software die wordt gebruikt in een verder 'leeg' besturingssysteem waarin alleen primaire software is geïnstalleerd (browser, e-mail, etc.).

Internet Veiligheidspakket voor Mobiele apparaten:

Het Mobiele Internet Veiligheidspakket wordt ondersteund door de volgende mobiele apparaten:

S60 3rd Edition (Symbian 9.x):

Nokia 3250, 5500, 5700, 6110, 6120, 6290, E50, E51, E60, E61, E61i, E62, E65, E70, E90, N71, N73, N75, N76, N77, N80, N81, N82, N91, N92, N93, N93i, N95, N95 8GB

S80:

Nokia 9300, 9300i, 9500

UIQ:

Sony Ericsson P1i, W950i, M600i, P990i, W960i

S60 2nd Edition (Symbian 7.x / 8.x):

Nokia 3230, 6260, 6600, 6630, 6670, 6680, 6681, 6682, 7610, N70, N72, N90, Panasonic X700, Panasonic X800

Windows Mobile 5.0 for Pocket PC: (ondersteunt ook devices zonder telefoonfunctionaliteit)

- Dopod 838, Dopod 900, Dopod 818 Pro
- HTC Prophet, HTC P3300, HTC P3350, HTC P3600, HTC P3300, HTC P3600, HTC P4350, HTC X7500 (Athene) HTC
- TyTN, HTC Universal, HTC Wizard, HTC X7500
- I-mate K-JAM, I-mate JASJAR, I-mate JAMin
- O2 Germany XDA neo, O2 Xda Atom, O2 Xda Exec, O2 XDA Mini S
- Qtek 9000, Qtek 9100, Qtek S200, Qtek v1640
- SPV M3000, SPV M5000, SPV M600

- T-Mobile MDA, MDA Pro, MDA Vario
- Asus P525, Cingular 8125, Gigabyte g-Smart, I-mate JAMin, Treo 700W, UBiQUIO 401, Palm Treo 750W, Toshiba Portégé G900

Windows Mobile 5.0 for Smartphone:

- HTC Faraday, HTC S310, HTC S620, HTC Tornado
- Qtek 8300, Qtek 8310
- Cingular 2125, I-mate SP5, I-mate SP5m Music Smartphone, Samsung SGH-i600, Samsung SGH-i320, T-Mobile MDA II Music, Toshiba Portege G500

Windows Mobile 6 Professional:

HTC P3450 (Touch), HTC Touch Dual, HTC Touch Cruise, HTC TyTN II (Kaiser)

Windows Mobile 6 Standard:

HTC S730, HTC S710

4 Service Level Agreements

4.1 Openstellingtijden Business Servicedesk

De Business Servicedesk van KPN ondersteunt de klanten. De Business Servicedesk is geopend op werkdagen van 08:00 tot 18:00 uur. Op officieel erkende Feestdagen is de Business Servicedesk van KPN gesloten.

KPN onderkent de volgende Feestdagen: Koninginnedag, 5 mei (éénmaal per vijf jaar), eerste en tweede Paasdag, Hemelvaartsdag, eerste en tweede Pinksterdag, eerste en tweede Kerstdag en Nieuwjaarsdag.

4.2 Beschikbaarheid

De dienst Internet Veiligheidspakket wordt 24 uur x 365 dagen aangeboden. KPN garandeert een minimale Beschikbaarheid (B) van 99%. KPN streeft ernaar om Incidenten en Problemen uiterlijk binnen 3 werkdagen op te lossen.

Het oplossen van Incidenten en Problemen, waarbij de dienstverlening zelf wel beschikbaar blijft, wordt niet meegeteld in de tijd dat de dienst niet beschikbaar is.

Het uitlopen van Gepland Onderhoud wordt wel meegeteld als tijd dat de dienst niet beschikbaar is.

Uitgesloten Uren (UU) maken geen deel uit van de berekening. Uitgesloten Uren (UU) zijn de uren waarop de dienstverlening niet beschikbaar is voor u en waarvan de oorzaak niet is toe te schrijven aan KPN. Deze storingen kunnen zijn:

- Storingen op het internet/publieke netwerk
- Storingen die worden veroorzaakt door componenten die niet vallen onder de dienstverlening en die niet vallen binnen verantwoordelijkheid van KPN
- Storingen die worden veroorzaakt door misbruik van de dienstverlening door u of uw Eindgebruikers
- Calamiteiten

4.3 Maintenance Window

Gepland Onderhoud zal plaatsvinden tijdens het Maintenance Window, op woensdag van 02:00 tot 07:00 uur, nationale feestdagen uitgezonderd. Indien hierop een uitzondering noodzakelijk is, worden hierover met u afspraken gemaakt.

De tijd dat de dienst niet beschikbaar is door Gepland Onderhoud neemt maximaal 8 uur per maand in beslag.

5 Helpdesk ingang en procedure

5.1 Openstellingstijden Business Servicedesk

Incidenten, Problemen en andere meldingen kunnen op één van de volgende manieren worden aangemeld:

- Per telefoon 0800-0403 (alleen tijdens openingstijden van de Business Servicedesk van KPN)
- Per e-mail onlinediensten@kpn.com
- Per fax (040) 299 88 59

5.2 Communicatie omtrent onderhoud

Wanneer tijdens Gepland Onderhoud een Wijziging wordt doorgevoerd waarbij de dienst functioneel wijzigt, dan stelt KPN u tenminste 15 werkdagen van tevoren op de hoogte.

5.3 Escalaties

Bij Escalaties zal de volgende communicatielijn binnen KPN gevolgd worden:

- Business Servicedesk van KPN
- Servicemanager van de dienst Internet Veiligheidspakket
- Productmanager van de dienst Internet Veiligheidspakket
- General Managers van KPN

Een Escalatie kan gestart worden als:

- Het overeengekomen Service Level niet gehaald worden
- Een nieuw Probleem zich voordoet dat niet is beschreven in de SLA
- Een Incident een grote impact heeft voor uw bedrijfsproces

Na constatering van een Escalatie zal de Business Servicedesk de communicatie verzorgen tussen betrokken partijen. De Servicemanager van de dienst Internet Veiligheidspakket zal een coördinerende rol innemen.

6 Facturatie

6.1 Tariefstructuur

De tarieven voor de dienst Internet Veiligheidspakket bestaat uit een maandelijks tarief.

6.2 Facturering

Facturering van de dienst Internet Veiligheidspakket geschiedt maandelijks achteraf. Betalingen dienen plaats te vinden in Euro's en binnen een termijn van 30 dagen.

6.3 Contractsduur

De standaard contractduur voor het Internet Veiligheidspakket is 1 jaar en wordt automatisch met 1 jaar verlengd. De opzegtermijn is 3 maanden. Een upgrade van de dienst gaat gepaard met een contractverlenging van een jaar.

U dient schriftelijk de dienst te beëindigen. De opzegging dient verzonden naar:

KPN
Abonnementsbeheer Software Online
Postbus 15
6400 AD HEERLEN
Fax: +31 (0)10 264 46 16
E-mail: onlinediensten@kpn.com

7 Informatiebeveiliging

Inleiding

KPN hanteert voor de beveiliging van zijn diensten, organisatie en infrastructuur de internationaal erkende standaard voor informatiebeveiliging ISO 27001 en ISO 27002 als richtlijn. Door het regelmatig (laten) uitvoeren van informatiebeveiligingscontroles, verificatie en in- en externe audits houdt KPN zijn informatiebeveiligingsniveau hoog.

7.1 De ISO 27001 en ISO 27002 richtlijn hoe te implementeren

De ISO 27001 beschrijft hoe een organisatie het managementsysteem voor informatiebeveiliging dient in te richten. In de bijlage van de ISO 27001 worden alle 133 ISO beheersmaatregelen omschreven. In de ISO 27002 worden de praktijkmethoden (best practices) voor implementatie van deze beheersmaatregelen aangegeven.

De 133 beheersmaatregelen zijn verdeeld over de volgende 11 aandachtsgebieden:


1. Beveiligingsbeleid
2. Organisatie van informatiebeveiliging
3. Beheer van bedrijfsmiddelen
4. Beveiliging van personeel
5. Fysieke beveiliging en beveiliging van de omgeving
6. Beheer van communicatie- en bedieningsprocessen
7. Toegangsbeveiliging
8. Verwerving, ontwikkeling en onderhoud van informatiesystemen
9. Beheer van informatiebeveiligingsincidenten
10. Bedrijfscontinuïteitsbeheer
11. Naleving

7.2 Continuïteitsbeheer

KPN beschikt over diverse continuïteitsplannen en over een afdeling crisismanagement. De continuïteitsplannen worden regelmatig geoefend en getest en zijn periodiek onderwerp van een interne/externe audit. Het doel hiervan is risico's te beperken en het borgen van een efficiënt en effectief herstel van onze dienstverlening in geval van een eventuele crisis.

Voor het implementeren van een solide continuïteitsproces hanteert KPN de internationaal erkende standaard BS 25999 als richtlijn.

7.3 Beveiligingsmaatregelen



Maar u kunt zelf ook een belangrijke bijdrage leveren aan het beveiligen van uw informatiestromen en (elektronische) persoonsgegevens. Denk hierbij bijvoorbeeld aan uw gebruikersnaam en wachtwoord of het beveiligen van uw interne draadloze netwerk. Wij adviseren u daarom om zelf ook effectieve beveiligingsmaatregelen te treffen. Dit kan bijvoorbeeld door een erkende installateur in te schakelen. Voor tips en aanvullende informatie kunt u terecht op onze site:

<http://www.kpn.com/zakelijk/service/veilig-internetten.htm>

Of kijk welke diensten KPN aanbiedt op het gebied van (internet)veiligheid:

<http://www.kpn.com/zakelijk/Meer-diensten.htm>