Dienstbeschrijving
Internetveiligheidspakket Protection Service for Business van F-Secure

Een dienst van KPN ÉÉN

Versie : v1.0
Datum : 1 januari 2018

Inhoud

1 Dit is Protection Service for Business van F-Secure

Tegenwoordig is het uitwisselen van gegevens en data via internet niet meer weg te denken uit ons dagelijks leven. Omdat u geen waardevolle data wilt verliezen, is beveiliging van uw apparaten tegen malware, phishing en hackers cruciaal.

Ongeautoriseerde toegang tot bedrijfssystemen heeft vaak (hoge) bedrijfskosten tot gevolg. Een aantal voorbeelden:

- Gestolen bedrijfsgevoelige informatie over bijvoorbeeld uw klanten kan juridische gevolgen hebben
- Criminelen kunnen aangetaste bedrijfssystemen gebruiken om frauduleuze betalingen te doen
- Verlies van persoonlijke- of bedrijfsgegevens kan leiden tot oplichting
- Versleuteling van uw bestanden (ransomware) leidt tot omkoping en/of dataverlies

Met het internet veiligheidspakket Protection Service for Business van F-Secure surft en downloadt u veilig op internet. Ook beschermt u uw data en uw bedrijfsmiddelen tegen dreigingen.

1.1 F-Secure

Zoals u van ons gewend bent, stellen we kwaliteit voorop. Daarom werken we samen met de hoogwaardige beveiligingssoftware van F-Secure.

1.2 Verschillende pakketten

- Protection Service for Workstation: voor de beveiliging van uw computer en/of Mac
- Protection Service for Mobile: voor de beveiliging van uw Android tablet of smartphone
- Protection Service for Server: voor de beveiliging van uw Windows Server
- Of een combinatiepakket: voor de beveiliging van uw computer en van uw smartphone/tablet

In deze dienstbeschrijving vindt u informatie over de functionaliteiten van het pakket dat u hebt gekocht. Hebt u een combinatiepakket aangeschaft? Lees dan hoofdstuk 2 en 3.

2 Computer en Mac

Criminelen bouwen tegenwoordig zeer geavanceerde malware. Zo kunnen ze van buitenaf binnendringen in uw computer. Verouderde software of het ontbreken van goede beveiligingsoplossingen kan kwetsbaarheden in uw bedrijfssystemen veroorzaken. Wist u bijvoorbeeld dat u 83% van de top 10-malware kunt vermijden met up-to-date software? En dat 87% van de zakelijke computers kritische updates missen? Eén van de functionaliteiten van het internetveiligheidspakket is het up-to-date houden van de software die u gebruikt.

2.1 Functionaliteiten

De functionaliteiten van Protection Service for Business Workstation zijn:

	Windows pc	Mac
Antivirus/malware/spyware	Ja	Ja
Browser Protection	Ja	Ja*
Firewall	Ja	Nee**
DeepGuard	Ja	Ja
Url-filtering	Ja	Ja
Software Updater	Ja	Nee
Beheerportaal	Ja	Ja

* alleen in Safari, **Firewall van OS X
Tabel 1: Functionaliteiten

Malware-, virus- en spywarebeveiliging

Het pakket detecteert en blokkeert schadelijke software (malware) die uw computer aanvalt. Dat kan via e-mail of verwisselbare media. Of als u materiaal van internet downloadt. Het pakket beschermt uw computer door de geïnstalleerde schadelijke software te verwijderen.

Firewall

Beschermt uw computer tegen ongeautoriseerde pogingen om een verbinding tot stand te brengen.

Browser Protection

Geeft aan of de website die u bezoekt veilig is. Als de website als verdacht of schadelijk wordt gezien, krijgt u een melding op uw scherm. Zo voorkomt u bijvoorbeeld dat u uw gegevens achterlaat op een schadelijke website, waardoor deze in handen komen van hackers. Dit wordt ook wel phishing genoemd.

DeepGuard

Analyseert de inhoud van bestanden en het gedrag van programma's. Er wordt voortdurend proactief op wijzigingen in software gecontroleerd. Daarmee bekijkt deze functionaliteit of er afwijkingen zijn van het standaardgedrag. Ook worden nieuwe en onbekende virussen, wormen en andere schadelijke programma’s geblokkeerd.

Software Updater

Scant computers op ontbrekende software-updates. Ook houdt het Windows en software van derden (bijvoorbeeld Adobe) up-to-date en vrij van kwetsbaarheden. Door steeds de nieuwste softwareversie te hebben, hebt u minder kans op beveiligingslekken en dus op malware. U kunt kiezen voor automatische of handmatige updates.

Beheerportaal

Met deze website kunt u de apparaten beheren die u beveiligt met het internetveiligheidspakket. U kunt profielen toekennen aan computers en controleren wat de beveiligingsstatus is. Het beheerportaal maakt standaard onderdeel uit van het pakket die u zelf in de zelfservice portal kan aanmaken.

Technische aspecten

Het internetveiligheidspakket voor **Windows** ondersteunt:

Besturingssystemen:

- Windows 7 met SP1 of hoger - alle 32-bit en 64-bit edities
- Windows 8 en 8.1 alle 32-bit en 64-bit edities
- Windows 10

Het internetveiligheidspakket voor **Mac (MacOS)** ondersteunt:

Besturingssystemen:

- OS X versie10.12 'Sierra'
- OS X versie10.11 'El Capitan'
- OS X versie10.10 'Yosemite'

3 Smartphone en tablet

Smartphones en tablets nemen steeds meer de functies van de computer over. Zo verwerken ze gegevens uit onder andere e-mails, documenten, apps en foto's. Beveiliging van smartphones wordt daarom ook steeds belangrijker. Malware, spyware, phishing op smartphones en tablets zijn geen uitzondering meer. Deze aanvallen zorgen voor onverwachte kosten en/of diefstal van persoonlijke gegevens. Het internetveiligheidspakket Protection Service for Business Mobile Security is beschikbaar voor Android smartphones en tablets.

3.1 Functionaliteiten

De functionaliteiten van Protection Service for Business Mobile zijn:

	Android smartphone en tablet
Browser protection	Ja
Anti-diefstal	Ja
Antivirus/malware	Ja
App scanning	Ja

Tabel 2: Functionaliteiten

Browser Protection

Geeft aan of de website die u bezoekt veilig is. Als de website wordt gezien als verdacht of schadelijk, krijgt u een melding op uw scherm. Zo voorkomt u bijvoorbeeld dat uw gegevens in handen komen van hackers. Dit wordt ook wel phishing genoemd.

Anti-diefstal

Kan op afstand het volgende met uw apparaat doen:

- geografisch lokaliseren
- alarm af laten gaan voor hoorbare vindbaarheid
- vergrendelen
- gegevens wissen
- een sms-waarschuwing naar de eigenaar sturen, als iemand de SIM-kaart in het toestel vervangt

Antivirus

Scant alle bestanden automatisch op virussen, malware en spyware. Dit gebeurt onder andere als deze worden opgeslagen, gekopieerd, gedownload of gesynchroniseerd. U kunt uw smartphone of tablet ook op elk gewenst moment handmatig op virussen scannen.

App scanning

Virussen en spyware worden steeds vaker via apps verspreid. Deze functionaliteit controleert hierop en zorgt ervoor dat de app die wordt gedownload ook de 'echte' app is.

Beheerportaal

Met deze website kunt u de apparaten beheren die u beveiligt met het internetveiligheidspakket. U kunt profielen toekennen aan smartphones en tablets. Ook kunt u controleren wat de beveiligingsstatus is. Het beheerportaal is een standaard onderdeel van het pakket pakket die u zelf in de zelfservice portal kan aanmaken.

Systeemvereisten

- Android smartphones en tablets met Android 5.0 en latere versies

- Besturingssysteem Android 5.1
- Vrije schijfruimte: 15 MB
- Internetverbinding: noodzakelijk om de laatste virusinformatie en updates te ontvangen

4 Servers

Zwakke plekken in uw serveromgeving maakt deze kwetsbaar voor aanvallen van buitenaf. Zo zijn e-mailservers bijvoorbeeld vaak het doelwit van deze aanvallen. Nadat u het internetveiligheidspakket Protection Service for Business Server Security op uw server hebt geïnstalleerd, zijn de bedrijfsgegevens en uw server beschermd tegen online bedreigingen.

4.1 Functionaliteiten

De functionaliteiten van Protection Service for Business Server zijn:

	Windows pc
Antivirus/malware/spyware	Ja
Browser Protection	Ja
DeepGuard	Ja
Software Updater	Ja
Beheerportaal	Ja

Tabel 3: Functionaliteiten

Malware-, virus- en spywarebeveiliging

Detecteert en blokkeert schadelijke software (malware) die uw server kan aanvallen. Het beschermt uw privacy door de geïnstalleerde schadelijke software van uw server te verwijderen. De gevonden malware wordt in quarantaine gezet of direct verwijderd. U kunt dit ook handmatig doen.

Browser Protection

Geeft aan of de website die u bezoekt veilig is. Als de website wordt gezien als verdacht of schadelijk, krijgt u een melding op uw scherm. Zo voorkomt u bijvoorbeeld dat uw gegevens in handen komen van hackers. Dit wordt ook wel phishing genoemd.

DeepGuard

Analyseert de inhoud van bestanden en het gedrag van programma's. Er wordt voortdurend proactief op wijzigingen in software gecontroleerd. Daarmee bekijkt deze functionaliteit of er afwijkingen zijn van het standaardgedrag. Ook worden nieuwe en onbekende virussen, wormen en andere schadelijke programma’s geblokkeerd.

Software Updater

Scant computers op ontbrekende software-updates. Ook houdt het Windows en de software van derden (bijvoorbeeld Adobe) up-to-date en vrij van kwetsbaarheden. Door steeds de nieuwste softwareversie te hebben, hebt u minder kans op beveiligingslekken en dus op malware. U kunt kiezen voor automatische of handmatige updates.

Beheerportaal

Met deze website kunt u de apparaten beheren die u beveiligt met het internetveiligheidspakket. U kunt profielen toekennen aan servers en controleren wat de beveiligingsstatus is. Het beheerportaal is een standaard onderdeel van het pakket die u zelf in de zelfservice portal kan aanmaken.

Technische aspecten

Protection Service for Business Server Security werkt voor Microsoft Exchange, Terminal Servers/Citrix, SharePoint Servers en EMC CAVA servers. Daarnaast hebt u nodig:

- Computers die aan de vereisten voldoen van het ondersteunde besturingssysteem

- 2 GB of meer schrijfruimte is aanbevolen
- Een internetverbinding voor updates en om Cloud-based detectie te kunnen gebruiken

U kunt het programma installeren op een server met de volgende Microsoft® besturingssystemen:

- Windows Server 2008
- Windows Server 2008 R2
- Small Business Server 2008
- Small Business Server 2011 Standard edition
- Small Business Server 2011 Essentials
- Windows Server 2012
- Windows Server 2012 Essentials
- Windows Server 2012 R2
- Windows Server 2012 R2 Essentials

Belangrijke informatie

- Op alle besturingssystemen moet de laatste update (Service Pack) geïnstalleerd zijn
- Voor een zo goed mogelijke werking en vanwege veiligheidsredenen werkt de dienst alleen op NTFS-partities
- Houd uw besturingssysteem up-to-date en gebruik alleen Windows-versies die beveiligingsupdates van Microsoft ontvangen. Het meest recente besturingssysteem heeft namelijk de beste beschermingstechnologieën.