KOCHCONSULTANCY
Security- & Privacy Awareness

proofpoint®

Proofpoint Essentials

“Enterprise-class” cyber-bescherming voor het MKB

Final – 22 Feb 2022

Cybercriminaliteit

MKB loopt dezelfde risico's als grote bedrijven

Cybercriminelen richten zich tegenwoordig met hun activiteiten steeds meer op de mens. Aanvallers gebruiken dezelfde tools als u: E-mail, social media en mobiele apparatuur. Onderzoek wijst bijvoorbeeld uit dat méér dan 90% van de cyber-aanvallen is gestart met het sturen van een phishing bericht naar particulieren, medewerk(st)ers van bedrijven en organisaties. In die phishing berichten maken cybercriminelen gebruik van slimme methodes om mensen te verleiden op een (valse) link in een e-mail te klikken of om een (besmette) bijlage van de e-mail te openen.

De gevolgen

De gevolgen van cybercriminaliteit kunnen groot zijn. Als een slachtoffer bijvoorbeeld onbewust zijn/haar inlog-gegevens invoert op een nagemaakte inlog-pagina kunnen de cybercriminelen vervolgens met die verkregen inlog gegevens toegang krijgen tot de systemen van het slachtoffer. Maar er kan ook kwaadaardige software worden geïnstalleerd waarmee in het ergste geval (als het om ransomware gaat) alle bedrijfsgegevens compleet "op slot" worden gezet waardoor het hele bedrijf stil komt te liggen. Pas na het betalen van een aanzienlijk bedrag aan losgeld (= ransom) beloven de criminelen dan om de gegevens weer toegankelijk te maken.

Hoe kunnen we weerbaar worden tegen deze bedreigingen?

E-mail is belangrijk voor iedere organisatie. We kunnen niet meer zonder. Het is wereldwijd geaccepteerd, iedere particulier, bedrijf of organisatie maakt er gebruik van. E-mail is daarom ook een belangrijk medium voor cybercriminelen om hun aanvallen uit te voeren.

De weerbaarheid tegen cybercriminaliteit kan vergroot worden door bedrijven te helpen bij:

- De bescherming van de E-mail systemen tegen inkomende E-mails die geïnfecteerde attachments (bijlagen) met malware, virussen of geïnfecteerde URL-links bevatten
- De bescherming tegen verlies van gegevens doordat vertrouwelijke informatie onbeschermd (niet-encrypted) wordt verstuurd
- De vergroting van het bewustzijn van medewerk(sters) door middel van aanval-simulaties (phishingtesten) en de juiste training aan de juiste mensen
- Het beschermen van Social Media accounts

Kennismaking met Proofpoint

Proofpoint, Inc. is een beveiligingsbedrijf dat “software als een service” (SAAS) producten levert voor e-mailbeveiliging, preventie van gegevensverlies en e-mailarchivering. Ze hebben meer dan 3.600 medewerk(st)ers en duizenden klanten verspreid over de wereld. In 2012 is het bedrijf naar de beurs gegaan, in 2020 was de omzet meer dan 1 Miljard USD.

Proofpoint Nexus Threat Intelligence Platform

Proofpoint voert de afgelopen jaren op dagelijkse basis miljarden security-analyses uit voor duizenden gebruikers. De kennis die hierbij wordt opgedaan over de oude en de meest moderne cyber-dreigingen wordt opgeslagen op het “Proofpoint Nexus Threat Intelligence Platform” en beschikbaar gemaakt voor alle Proofpoint-gebruikers. In de loop van de afgelopen jaren is op dat platform door middel van AI (Artificial Intelligence) en machine learning een enorme hoeveelheid kennis (intelligence) opgebouwd over cyber-dreigingen.

De kennis op het Proofpoint platform over aanvallen en cyber-risico’s wordt continu bijgewerkt met informatie die wordt verkregen uit de real-time analyses die 24/7 worden uitgevoerd bij de Proofpoint gebruikers. Om een idee te krijgen over de hoeveelheid analyses:

- Er worden dagelijks 200+ miljoen attachments (e-mail bijlagen) geanalyseerd
- Er gaan dagelijks 17+ miljoen attachments (e-mail bijlagen) door een sandbox-analyse
- Er worden dagelijks 26+ **miljard** URL’s geanalyseerd op kwaadaardige elementen
- Er worden dagelijks 22+ miljoen cloud accounts gemonitord
- Er worden dagelijks 2,2+ **miljard** e-mail berichten geanalyseerd op kwaadaardige elementen

De kennis die Proofpoint heeft opgebouwd op het “Proofpoint Nexus Threat Intelligence Platform” wordt ingezet voor de bescherming van de gebruikers. Op deze manier zijn de gebruikers er zeker van dat ze worden beschermd tegen de meest actuele cyber-aanvallen.

Proofpoint Essentials

"Enterprise-class" cyber-bescherming voor het MKB

Wat is Proofpoint Essentials?
Proofpoint Essentials is een kostenbesparende en eenvoudig te gebruiken security oplossing die speciaal is ontwikkeld voor het Midden- en kleinbedrijf. Proofpoint Essentials is een SAAS (Software as a Service) oplossing. Er hoeft dus geen hardware of software geïnstalleerd te worden en de updates worden automatisch uitgevoerd.

Dezelfde bescherming als grote organisaties
Ieder MKB bedrijf heeft te maken met dezelfde cyber-dreigingen als grote organisaties. Proofpoint Essentials maakt daarom gebruik van dezelfde kennis over cyber-dreigingen, beschikbaar gesteld via het Proofpoint Nexus Intelligence Platform. Met Proofpoint Essentials krijgen de gebruikers uit het MKB daarom dezelfde bescherming als grote bedrijven.

Er zijn voor Proofpoint Essentials twee belangrijke onderdelen beschikbaar waarmee bescherming geboden wordt tegen cyber-dreigingen. Deze twee onderdelen zijn:

1. **Proofpoint Essentials (E-mail security en databescherming)**

Proofpoint Essentials biedt het MKB dezelfde bescherming tegen cyber-dreigingen als grote, zéér security-bewuste organisaties:

- Uitgebreide cybersecurity met spam- en phishing -detectie
- Dynamische sandboxing van attachments (bijlagen) en URL's
- E-mail encryptie en DLP (Data Loss Prevention)
- Social Media account bescherming

2. **Proofpoint Essentials Security Awareness**

Geen enkele cybersecurity oplossing is compleet als er geen rekening wordt gehouden met het bewustzijn van de mensen in de organisatie. Met de Security Awareness component van Proofpoint Essentials krijgt u Security Awareness training voor alle medewerk(st)ers. Het helpt bij het verlagen van de risico's van phishing aanvallen en malware infecties. Het maakt uw medewerk(st)ers weerbaar en dat verlaagt het aantal security incidenten en datalekken.

- Met de ThreatSim phishing simulaties (phishingtesten) krijgt u inzicht in de gevoeligheid van de organisatie voor phishing
- Er is aansprekende training content (E-learning) beschikbaar in 40+ talen
- Uitgebreide rapportages geven duidelijkheid over het gedrag van medewerk(st)ers bij gesimuleerde aanvallen

Beide onderdelen (1 en 2) kunnen los van elkaar gebruikt worden.
Als beide onderdelen in de organisatie worden gebruikt krijgt u de beste waarde voor uw investering: Sterke bescherming tegen cyber-aanvallen **PLUS** Security Awareness training waarmee medewerk(st)ers (en dus uw organisatie) weerbaar worden tegen dreigingen.
Hieronder kunt u meer informatie lezen over de twee bovengenoemde onderdelen.

1. Proofpoint Essentials
(E-mail security en databescherming)

Het eerste onderdeel zoals hierboven omschreven is Proofpoint Essentials Advanced.

Met Proofpoint Essentials Advanced wordt E-mail security en databescherming geboden. Het verdedigt de organisatie tegen cyberdreigingen zoals virussen, spam, phishing, ransomware en E-mail fraude. Door de makkelijk te gebruiken en intuïtieve user interface krijgen de beheerders een goed inzicht in de cyber-dreigingen die gericht zijn op de organisatie. Met deze kennis wordt de besluitvorming omtrent de benodigde security maatregelen effectiever.

Met geavanceerde scanners worden alle e-mail berichten snel gescand en worden alle bekende virussen geblokt. Om de bescherming nog sterker te maken wordt er ook gebruik gemaakt van “heuristics” scanning methodes om verdachte situaties te herkennen. Zo’n verdachte situatie zou immers ook een nog niet ontdekt virus of e-mail dreiging kunnen zijn.

Uitgebreide bescherming tegen cyberdreigingen
De meeste cyber-aanvallen worden uitgevoerd op mensen. E-mail speelt hier een belangrijke rol in. De slachtoffers worden verleid om op een link te klikken of om een attachment (bijlage) te openen.

Proofpoint Essentials haalt deze zorg bij u weg door middel van “Targeted Attack Protection (TAP)”. TAP is een unieke Sandbox-technologie voor URL’s en attachments (bijlagen) waarmee continu (nieuwe) aanvallen worden gedetecteerd. Het geeft inzicht in welke mensen binnen de organisatie de meeste kans lopen om aangevallen te worden.

Data Loss Prevention (DLP) en filtering van content
Proofpoint Essentials helpt organisaties compliant te blijven. Met behulp van een beleid gestuurde DLP filter wordt gevoelige informatie in e-mails automatisch herkend en beschermd. Hierbij wordt gebruik gemaakt van ingebouwde term-woordenboeken en intelligente zoekmachines (SmartSearch identifiers). Gevoelige informatie kan bijvoorbeeld de volgende informatie bevatten:

- Persoonsgegevens
- Medische gegevens
- Financiële gegevens
- AVG-gegevens

Zie voor een (Engelstalige) beschrijving van Proofpoint Essentials E-mail Security:
https://www.proofpoint.com/sites/default/files/pfpt-us-ds-essentials-advanced-package.pdf

Automatische E-mail encryptie

Er wordt veel vertrouwelijke informatie via E-mail uitgewisseld, zowel intern (bijv. tussen vestigingen) als met relaties, partners en klanten. E-mails die gevoelige informatie bevatten dienen goed beschermd te worden om datalekken en de daarbij horende financiële-, operationele- en reputatieschade te voorkomen. Medewerk(st)ers kunnen vertrouwelijke informatie onbeschermd versturen. Zonder de juiste security procedures loopt u daarbij de kans op datalekken. Met de Proofpoint Essentials E-mail encryptie voorkomt u mogelijke negatieve gevolgen ten gevolge van dataverlies.

Proofpoint Essentials E-mail encryptie biedt de volgende functionaliteit:

- U kunt filters definiëren die automatisch uitgaande E-mails identificeert die beveiligd (encytpted) moeten worden. Zodra er gevoelige informatie wordt ontdekt wordt de E-mail automatisch beveiligd met encryptie
- Gebruikers kunnen zelf hun uitgaande e-mails encrypten door middel van een eenvoudige “tag” in het onderwerp van de E-mail
- Uw interne gebruikers kunnen encrypted E-mails maken, lezen en beantwoorden
- Externe gebruikers kunnen gebruik maken van een secure, web-based interface waarmee de encrypted E-mails die ze ontvangen kunnen worden gelezen en worden beantwoord

Voor meer (Engelstalige) informatie over E-mail encryptie:
https://www.proofpoint.com/sites/default/files/pfpt-us-ds-essentials-email-encryption.pdf

Business Continuity

E-mail neemt een belangrijke plaats in bij de dagelijkse activiteiten van elke organisatie. Het wegvallen van het E-mail systeem zal al op korte termijn grote problemen veroorzaken. Proofpoint Essentials (Advanced) biedt de volgende functionaliteit om ervoor te zorgen dat uw E-mail communicatie altijd beschikbaar is bij een crisis situatie:

- E-Mail spooling: Indien uw E-mail server crasht, of als er netwerk problemen zijn waardoor de connectie met uw E-mail server wegvalt zorgt Proofpoint Essentials ervoor dat uw inkomende E-mail automatisch wordt bewaard op een backup server.
- Inbox voor noodgevallen: Bij het uitvallen van het e-mail systeem kunt u toch gebruik blijven maken van E-mail door middel van de speciale Inbox voor Noodgevallen. Zodra de connectie met de E-mail server weer hersteld is worden de E-mails automatisch teruggezet vanaf de backup server
- Instant replay: Gebruikers kunnen elke e-mail gedurende een periode van 30 dagen nogmaals verzenden.

Zie voor meer (Engelstalige) informatie over de inbox voor noodgevallen:
https://www.proofpoint.com/sites/default/files/ppe_emergency_inbox_customer-a4-cm.pdf

Social Media account bescherming

Proofpoint Essentials (Advanced) helpt u bij het beschermen van maximaal 3 accounts op Social Media. U kunt kiezen uit Facebook, Twitter, Youtube. De accounts worden gemonitord op cyber-aanvallen en beschermd tegen spam en malware die op uw kanalen worden geplaatst.

Er zijn drie abonnementen beschikbaar, voor elk van de twee segmenten (0-250 gebruikers en 250-1000 gebruikers)		Business	Advanced	Pro
Core Bescherming	Anti-Spam/Anti-Virus	✓	✓	✓
	Filteren van aangepaste inhoud	✓	✓	✓
	Bescherming tegen nep-email's	✓	✓	✓
Gerichte aanval bescherming	URL-verdediging	✓	✓	✓
	Bijlageverdediging Reputatie	✓	✓	✓
	Bijlageverdediging Sandboxing			✓
	Bescherming Social Media Accounts		✓	✓
Bescherming van uitgaande aanvallen	Uitgaande filtering	✓	✓	✓
	Preventie van gegevensverlies	✓	✓	✓
	Encryptie van e-mail		✓	✓
Continuïteit	Inbox voor noodgevallen	30 dagen	30 dagen	30 dagen
	Spooling van e-mail	30 dagen	30 dagen	30 dagen
E-mail-archivering	Ondersteuning voor Exchange en Office365			✓
	Zoeken en vinden			✓
	Importeren & exporteren van data			✓

2. Proofpoint Essentials Security Awareness

(Security Awareness training en simulaties)

Zoals al eerder gezegd: geen enkele cybersecurity oplossing is compleet als er geen rekening wordt gehouden met het bewustzijn van de mensen in de organisatie. De ervaring leert ons dat meer dan 70% van de security incidenten wordt veroorzaakt door menselijk handelen. Cybercriminelen gebruiken slimme methodes om mensen om de tuin te leiden. Slachtoffers worden verleid om op een link te klikken of om een attachment te openen. Hierbij wordt misbruik gemaakt van normale menselijke eigenschappen zoals naïviteit, onwetendheid, eigenwijsheid of angst. De gevolgen voor de slachtoffers zijn groot. Denk hierbij aan financiële- , operationele- en reputatieschade en bij de slachtoffers komt ook veel schaamte voor.

Security Awareness training verhoogt de weerbaarheid

Met Proofpoint Essentials Security Awareness worden mensen bewust gemaakt van deze vormen van criminaliteit. Bewuste mensen zijn weerbaar en dat verlaagt het aantal security incidenten en datalekken. Security awareness training helpt mensen om phishing-activiteiten (via E-mail, SMS, Whatsapp, Social Media en telefonisch) te herkennen waardoor de kans op malware besmettingen wordt verlaagt.

Phishing simulaties en security awareness training

Proofpoint Essentials Security Awareness biedt de mogelijkheid om phishing simulaties uit te voeren en security awareness training te verzorgen aan medewerk(st)ers. Hiermee worden de medewerk(st)ers geleerd op de juiste manier om te gaan met cyber-dreigingen en op de juiste manier te reageren als er sprake is van een dreiging.

Met de ThreatSim phishing simulaties van Proofpoint kunt u de gevoeligheid van de organisatie peilen voor phishing aanvallen. Er zijn duizenden phishing templates beschikbaar in diverse categorieën. Deze phishing templates zijn verkregen vanuit het Proofpoint Nexus Threat Intelligence Platform. Met behulp van deze templates kunnen de volgende dreigingen worden gesimuleerd:

- Kwaadaardige attachments (E-mail bijlagen)
- Ingevoegde URL-links in een E-mail waarop de slachtoffers moeten klikken
- Verzoeken om persoonlijke en/of vertrouwelijke informatie in te voeren

Gebruikers die in een phishing simulatie trappen kunnen automatisch uitgenodigd worden voor het volgen van interactieve training (E-learning modules). Hierbij worden de gebruikers geleerd over de gevaren van phishing en hoe ze in de toekomst dergelijke phishing e-mails kunnen herkennen.

E-Learning bibliotheek

De bibliotheek van security-onderwerpen die worden behandeld tijdens de interactieve- en spel-gebaseerde trainingen wordt constant bijgehouden en up-to-date gemaakt. De lesstof behandelt een breed scala aan security risico's en is beschikbaar in meer dan 40 talen.
Alle modules zijn "on demand" beschikbaar, wat betekent dat de medewerk(st)ers de modules kunnen bekijken op een moment dat het hen het beste uitkomt. De modules zijn ook geschikt om te bekijken vanaf een mobiel apparaat. De schermindeling wordt dan automatisch aangepast. De modules duren tussen de 5 en 15 minuten. Dit is een kleine investering in tijd voor dit belangrijke onderwerp.

Analyseer de resultaten met rapportages

Proofpoint Essentials Security Awareness biedt duidelijke rapporten waarmee inzicht wordt verkregen in de voortgang en hoe de medewerk(st)ers aan het werk zijn met:

- Assessments
- Gesimuleerde aanvallen (Phishing simulaties)
- Training

Awareness vergroting is een continu proces

Een éénmalige activiteit is niet voldoende om de awareness van medewerk(st)ers te vergroten en ze te overtuigen van het nut en de noodzaak van veilig gedrag. Er zal dan snel worden "terug gevallen" naar het oude, onveilige gedrag.
Awareness vergroting vraagt om een continu proces van meten en leren en rapporteren. Proofpoint Essentials geeft u de mogelijkheid van een continu meet- en leerproces. Het geeft de kwetsbare plekken in de organisatie aan en levert gerichte training op die plekken waar het nodig is.

Proofpoint Essentials

Threat Protection Bundel

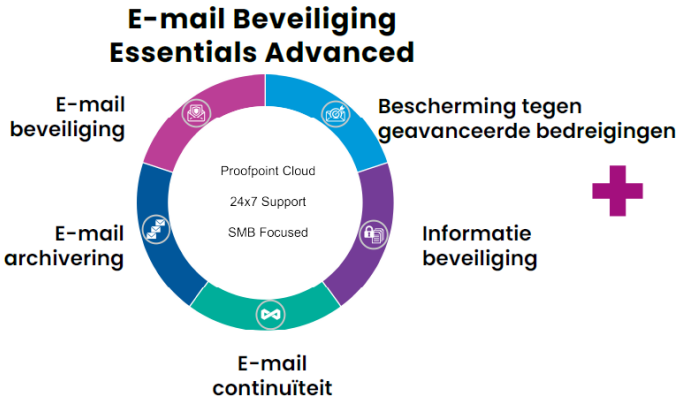
Binnen het Proofpoint Essentials portfolio zijn twee belangrijke Proofpoint onderdelen beschikbaar waarmee “Enterprise-class” bescherming geboden wordt tegen cyber-dreigingen die gericht zijn op systemen en mensen binnen het MKB.

- Proofpoint Essentials: E-mail security en databescherming
- Proofpoint Essentials Security Awareness : Training van medewerk(st)ers

Bundel
De twee onderdelen van Proofpoint Essentials kunnen los van elkaar gebruikt worden. Echter, U haalt het meest uit uw investering als beide onderdelen in de organisatie worden gebuikt.

Om dit voor het MKB extra aantrekkelijk te maken is de “Threat Protection Bundel” gemaakt. Hiermee kunt u tegen aantrekkelijk lage kosten gebruik maken van beide onderdelen.

- Sterke bescherming tegen aanvallen, phishing en malware
- Weerbare medewerk(st)ers door security awareness training
- Onbeperkt phishing simulaties uitvoeren
- Beide onderdelen eenvoudig te gebruiken vanuit dezelfde user-interface
- Lage kosten per medewerk(st)er



Security Awareness (PE-SA)	
Dreiging gebaseerde Intel via integratie	✓
ThreatSim Phishing	✓
Opleidingsmodules	45 modules (en groeiend)
Rapportage	Bedrijfstraining rapportkaart, Campagne geschiedenis (ThreatSim)
Aanpassing	Traiining E-mail Meldingen, ThreatSim Leerzame Momenten
Atomatische whitelisting van PE-SA e-mails	✓
User Management	✓
Multinationale ondersteuning	✓

Zie voor meer (Engelstalige) informatie over de Proofpoint Essentials Threat Protection bundel:
https://www.proofpoint.com/sites/default/files/data-sheets/pfpt-us-sb-essentials-threat-protection.pdf

Meer informatie?
Wilt u meer informatie over de voordelen van Proofpoint Essentials?
Wilt u een toelichting op de informatie in dit document
Wilt u een demonstratie van Proofpoint Essentials (online of bij u aan huis)
Wilt u een offerte aanvragen voor het afsluiten van een Proofpoint Essentials licentie?

Neem dan gerust contact op via onderstaande contactegevens

Contact informatie

Koch Consultancy BV
Beetzlaan 5
3762 CA Soest

Tel: 06-53233269

Website: www.kochconsultancy.nl
E-mail: info@kochconsultancy.nl

KOCHCONSULTANCY
Security- & Privacy Awareness