Een abonnement op veiligheid

DesktopToWork Security

DESKTOP TO WORK

DesktopToWork **Security**

Een abonnement op veiligheid

Ons zakelijk leven vindt steeds vaker online plaats. We bankieren online, betalen digitaal, streamen muziek en hebben toegang tot allerlei online-applicaties en data. We kunnen ons geen leven meer voorstellen zonder internet. Digitaal werken biedt echter niet alleen gemak, maar brengt ook risico's met zich mee.

De online wereld trekt criminelen, hackers en ongewenste mensen aan. Zij zijn continu op zoek naar mogelijkheden om jou en je organisatie te beroven, je (online) identiteit te stelen, fraude te plegen, en willen je grote sommen geld laten betalen om versleutelde data weer beschikbaar te krijgen of niet publiekelijk te publiceren. Daarom is digitale gegevensbeveiliging en cyberveiligheid van het grootste belang.

DesktopToWork helpt organisaties hun gegevensbeveiliging en cyberveiligheid te vergroten. Met behulp van een gedegen aanpak onderzoeken en analyseren we digitale kwetsbaarheden. Door het inzetten van de juiste tools en kennis op het vlak van cyberveiligheid kunnen we de risico's minimaliseren en potentiële kwetsbaarheden proactief beschermen.

In deze brochure gaan we uitgebreid in op digitale gegevensbeveiliging en cyberveiligheid. Ook geven we een gedetailleerde definitie van wat deze termen nu eigenlijk betekenen en hoe DesktopToWork jouw digitale informatie kan beveiligen.

DESKTOP TO WORK

Contact?

085-7605000
info@desktoptowork.com
www.desktoptowork.com

Laan van Waalhaven 277
2497 GL Den Haag

Wanneer?
Op werkdagen van 07:00 – 18:00

Partner Service Provider

Microsoft Tier-1 Cloud Soultions Provider

Gold Microsoft Partner

Cisco Select Partner

ISAE 3402 CERTIFIED

Managementsysteem certificate DNV ISO 27001

DTW Security

Laten we beginnen met de basis. Wat is digitale beveiliging?

Digitale gegevensbeveiliging is de term die wordt gebruikt om je zakelijke online identiteit en veiligheid alsmede je persoonlijke data en bedrijfsdata te beschermen. Dit is mogelijk met behulp van oplossingen zoals Microsoft 365, identiteit en toegangsbeheer, biometrische beveiliging, maar ook door middel van een gedegen back-up plan. Daarnaast is het van groot belang dat medewerkers de juiste vorm van educatie krijgen aangeboden en op de hoogte zijn van potentiële gevaren.

Wat is het verschil tussen digitale gegevensbeveiliging en cyberveiligheid?

De kans is groot dat je weleens gehoord hebt van de term "cyberveiligheid".
Toch is er een verschil tussen digitale gegevensbeveiliging en cyberveiligheid. Digitale gegevensbeveiliging omvat het beschermen van je online identiteit, je persoonlijke en bedrijfsdata en tevens al je bedrijfsgegevens. Cyberveiligheid bestrijkt meerdere terreinen. Het beschermt tevens je volledige netwerk, computersystemen en andere digitale componenten en de daarin opgeslagen gegevens tegen ongeoorloofde toegang. Digitale gegevensbeveiliging kun je dus zien als een subtype van cyberveiligheid. Veel professionals uit de industrie gebruiken de twee termen overigens gewoon door elkaar, maar in werkelijkheid is er een duidelijk onderscheid. Digitale gegevensbeveiliging beschermt informatie. Cyberbeveiliging beschermt zowel de infrastructuur, systemen, netwerken en informatie. DesktopToWork spreekt daarom altijd van cyberbeveiliging of cyberveiligheid.

Waarom is cyberveiligheid dan zo belangrijk?

Recent onderzoek wijst uit dat elke dag meer dan zeven miljoen systemen succesvol worden aangevallen en dat het aantal incidenten van cyberfraude en -misbruik in 2020 al met 20 procent is toegenomen. De wereldwijde kosten van cybercriminaliteit zullen de komende vijf jaar naar verwachting jaarlijks met 25% toenemen, tot 10.5 biljoen dollar per jaar in 2025. Ter vergelijking, in 2015 was dit 3 biljoen dollar.

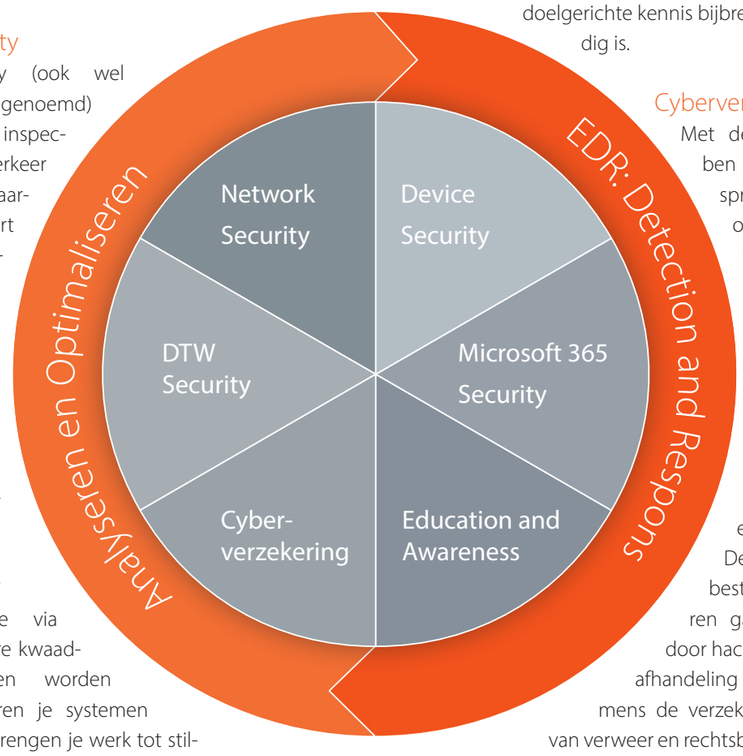
Cybercriminelen zijn opportunisten die worden aangetrokken door de enorme hoeveelheid en verscheidenheid aan gegevens die beschikbaar zijn voor uitbuiting en het geld dat ze hiermee kunnen verdienen. En alles wat ze nodig hebben, is slechts één schot in de roos om hun inspanningen de moeite waard te maken. Als ze slechts één organisatie voor de gek kunnen houden, bijvoorbeeld door middel van een phishing-aanval, kunnen hackers enorme schade aanbrengen aan een gestolen identiteit. Het wordt nog veel erger wanneer zij alle data van de organisatie versleutelen en geld vragen om deze data weer toegankelijk te maken.

Wat zijn de verschillende vormen van cyberbeveiliging?

DesktopToWork heeft zes pilaren gedefinieerd met betrekking tot cyberbeveiliging. Deze zes pilaren zijn de fundamentele bouwstenen als het gaat om de beveiliging van alle IT systemen. Daarnaast geloven wij dat het continue analyseren en optimaliseren van de online veiligheid van essentieel belang is. Cybercriminelen staan helaas nooit stil. Hiermee vormt DesktopToWork de zesde bouwsteen.

Network Security

Network security (ook wel edge-security genoemd) controleert en inspecteert internet verkeer van buitenaf. Daarnaast identificeert het geautoriseerde gebruikers, blokkeert het ongeautoriseerde toegang en beschermt het tegen virussen en malware van de nieuwste generaties.



Device Security

Bedreigingen die via malware en andere kwaadaardige systemen worden verspreid, infecteren je systemen en gegevens en brengen je werk tot stilstand. Met de juiste device security detecteer en verwijder je niet alleen deze infecties, maar het houdt ook verdachte programma's buiten en isoleert het waarschijnlijke bedreigingen. Als we spreken over device security dan betreft dit ieder type apparaat. Van Windows systemen tot ieder type mobiele telefoon.

Microsoft 365 Beveiliging

Met behulp van Microsoft 365 zorg je voor een gedegen beveiliging van al je cloud applicaties. Door middel van multi-factor authenticatie en toegangscontrole zorgen we ervoor dat jouw digitale identiteit beschermd is. Daarnaast kunnen we met behulp van Compliance beheer informatie op basis van importantie kwalificeren en beveiligen.

Education and Awareness

Cyberbeveiliging start altijd bij de eindgebruiker van een systeem. Door middel van periodieke kortstondige educatie met behulp van e-learnings, educatieve boekjes en vragenuren helpen wij medewerkers om zich beter te wapenen tegen bedreigingen van buitenaf. Zelf in staat zijn om bedreigingen te herkennen en te negeren, speelt hierbij een belangrijke rol. Tevens kunnen we gevraagd en ongevraagd cyberdreigingen "simuleren" en hiermee de eindgebruiker doelgerichte kennis bijbrengen indien dit nodig is.

Cyberverzekering

Met de cyberverzekering ben je naast de aansprakelijkheid van een onderneming ook voor aangebrachte schade door cybercriminelen, inclusief de daaruit voortvloeiende gevolgschade, verzekerd voor de eigen kosten naar aanleiding van een digitaal risico. Deze risico's kunnen bestaan uit het verloren gaan van gegevens door hacking of phising. Ook afhandeling van de schade namens de verzekerde en de kosten van verweer en rechtsbijstand zijn hiermee verzekerd.

DesktopToWork

Door middel van van 24/7/365 monitoring kan het DesktopToWork beveiligingsteam informatie verzamelen, problemen diagnosticeren en toezicht houden op alle IT systemen. DesktopToWork detecteert potentiële kwetsbaarheden en beheert eventuele zwakke plekken in het systeem van jouw organisatie. Met behulp van kwetsbaarheidsscanners identificeren we niet alleen gebreken, maar geven er ook prioriteit aan om je te helpen bij het organiseren van tegenmaatregelen.

Illustratie: De 6 Pilaren van Cyberbeveiliging

Network Security

Internet is ooit ontstaan door verschillende computers met elkaar te verbinden. Dat kleine netwerk groeide uit tot een wereldwijd web waar we zowel zakelijk als privé dankbaar gebruik van maken. Door de immense groei van het internetverkeer zijn er echter ook steeds meer cybercriminelen actief die hier misbruik van willen maken. Dat maakt het belang van beveiligde netwerken steeds groter. Netwerkbeveiliging is volop in ontwikkeling. Zo biedt de Next-generation firewall (NGFW) veel meer mogelijkheden dan een standaard netwerkbeveiliging.

Extra functies

Waar een standaard firewall inkomend en uitgaand netwerkverkeer filtert op basis van de IP-poort (Internet Protocol) en IP-adressen, voegt een firewall van de volgende generatie extra functies toe. Door het verkeer van netwerkpakketten intelligent te inspecteren, kunnen nieuwe verbindingsverzoeken worden geassocieerd met mogelijke cyberbedreigingen. De extra functies die de nieuwe generatie netwerkapparatuur heeft te bieden, zijn onder meer applicatiebeveiliging, geïntegreerde inbraakpreventie en geavanceerdere mogelijkheden voor het voorkomen van bedreigingen, zoals malware en ongeautoriseerde toegang.

Inbraakpreventie

Met IDS, dat staat voor intrusion dectection system, kun je regels instellen voor het verkeer dat wel en niet wordt toegelaten op het netwerk. Dit is geen overbodige luxe want elk netwerk is tegenwoordig een mogelijk doelwit voor aanvallen. Daarom is het belangrijk dat je aanvallen van tevoren kunt opsporen en vervolgens tegenhouden (detectie & preventie). Alle reeds bekende bedreigingen, zoals malware, staan opgeslagen in een database. Deze wordt dagelijks geactualiseerd zodat ook de nieuwste bedreigingen worden tegengehouden in het netwerk.

Geavanceerde Malware Protectie

Alleen blokkeren van malware is niet voldoende. Het is net zo belangrijk om een zo'n compleet mogelijk beeld te verkrijgen van je totale netwerkverkeer. Advanced Malware Protection (AMP) zorgt hiervoor. Het checkt direct elk gedownload bestand in een malware database en blokkeert automatisch reeds bekende bedreigingen. Het kan echter ook op een later tijdstip vaststellen dat een bestand een bedreiging blijkt te zijn. Dit is mogelijk omdat al het netwerkverkeer wordt gecontroleerd en bijgehouden in een database. Op die manier kan dus ook met terugwerkende kracht actie worden ondernomen om de bedreiging tegen te gaan.

Analyse van malware met Threat Grid

Het in AMP geïntegreerde Threat Grid analyseert wat de potentiële malware doet op het netwerk en vertaalt dit naar voor mensen leesbare rapporten. Hierbij worden 950 verschillende indicatoren gebruikt dat ook menselijk handelen nabootst.

Firewall op basis van locatie

De nieuwe generatie netwerkapparatuur kan ook worden gebruikt om verkeer te blokkeren op basis van het inkomend verkeer uit het land van herkomst of het uitgaand verkeer naar het land van bestemming. Je hebt dus de mogelijkheid om al het verkeer vanuit of naar bepaalde landen te blokkeren. Is het voor jouw organisatie bijvoorbeeld niet nodig om verkeer uit Rusland of China toe te staan, dan kun je dit eenvoudig aanpassen en blokkeren.

Webinhoud filteren

Met de nieuwe generatie netwerkapparatuur kun je op een geavanceerde manier inhoud filteren. Hiervoor selecteer je naar keuze een aantal categorieën of websites die je wilt blokkeren zodat ze voor medewerkers niet meer toegankelijk zijn op het bedrijfsnetwerk. Denk hierbij bijvoorbeeld aan online games en gok- of 18+ websites.

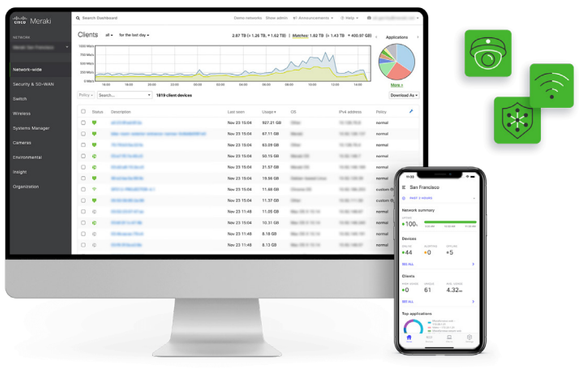
Deze websites zijn niet alleen slecht voor de productiviteit maar staan er ook om bekend dat ze vaak malware verspreiden. Zo kunnen de gebruikers van je netwerk blijven profiteren van de voordelen van het internet, maar zijn ze tegelijkertijd beschermd tegen ongepaste of schadelijke inhoud zonder dat dit ten koste gaat van de productiviteit.

Filteren van zoekopdrachten

Wanneer een apparaat toegang probeert te krijgen tot een webpagina, wordt het webadres vergeleken met een groot aantal URL's in een database. Dit maakt het mogelijk om bijvoorbeeld de toegang tot een specifieke URL op een website toe te staan, terwijl andere webadressen juist worden uitgesloten. Zo kunnen specifieke URL-adressen aan een witte lijst worden toegevoegd zodat ze niet worden geblokkeerd door de filter.

Overzichtelijk rapport

Het is heel belangrijk om precies te weten wat er allemaal gebeurt op je netwerk. Daarom sturen we je wekelijks of maandelijks een overzichtelijk rapport met alle potentiële aanvallen die zijn afgeslagen. In het rapport is te zien op welke vestiging dit is geweest, van welk land de aanval kwam, wat voor soort aanvallen het waren en zelfs welke apparaten en besturingssystemen het meest werden benaderd.



Meraki Dashboard

Device Security

Device Security:
Beveilig je lokale en online werkplek

Als je wilt voorkomen dat de apparaten in je bedrijfsnetwerk, zoals desktops, laptops en mobiele telefoons, een grote kans lopen om slachtoffer te worden van ransomware, malware of phishing mails, dan heb je een complete eindpuntbeveiliging nodig. Het is de oplossing om jouw organisatie en je medewerkers te beschermen tegen de gevaren die dit tegenwoordig met zich meebrengt. Apparaat beveiliging, ofwel device security verdient vandaag de dag alle aandacht van iedere organisatie die cyberbescherming serieus neemt. DesktopToWork biedt een complete beveiligingsoplossing voor zowel online als lokale eindpunt apparaten.

Bescherm je werknemers overal

Het idee dat het voltallige personeel van een bedrijf op dezelfde plek werkt, is al enige tijd door de werkelijkheid achterhaald. De coronacrisis heeft ons geleerd dat het (technisch) ook heel goed mogelijk is om thuis te werken. Hoewel thuiswerken na het post-corona tijdperk minder massaal zal worden gepraktiseerd, is het idee dat je ook buiten het bedrijfspand uitstekend kunt werken niet meer weg te denken uit de moderne samenleving. Ook voor de crisis waren er al tal van initiatieven op dat gebied. Daarnaast is ook de werknemer die vooral onderweg zijn werkzaamheden uitvoert, een factor van belang geworden.

De zwakste schakel

Al je medewerkers, of ze nu thuis, op kantoor of onderweg zijn, maken continu een verbinding met het centrale bedrijfsnetwerk. De apparaten (devices) die zij daarbij gebruiken worden beschouwd als een eindpunt. Je moet er dus voor zorgen dat je medewerkers overal beschermd zijn. Met andere woorden: eindpunt apparaten hebben een sterke beveiliging nodig. Niet zelden zijn ze de zwakste schakel in de netwerkbeveiliging en een gemakkelijke prooi voor cybercriminelen.

Wat is ransomware?

Ransomware is een speciale vorm van malware en vormt een ernstige bedreiging voor jou en je apparaat. Het Engelse woord ransom betekent losgeld. Dat is precies wat deze afpersingssoftware doet zodra het eenmaal op jouw apparaat terecht is gekomen. Het vergrendelt het besturingssysteem of versleutelt belangrijke bestanden en geeft je pas weer toegang als je daar een flink bedrag voor betaalt. Diverse grote ondernemingen hebben hier mee te maken en betalen soms stilzwijgend het losgeld. De top 5 van bedrijven in de Verenigde Staten die werden getroffen door ransomware moesten bedragen tussen de 1,14 en 4,5 miljoen US dollar ophoesten om weer toegang te krijgen tot hun netwerk.

Eindpuntbeveiliging van DesktopToWork

DesktopToWork biedt voor zowel de online werkplek als lokale computers een complete beveiligingsoplossing voor eindpunten aan die bescherming biedt tegen de meest voorkomende gevaren zoals ransomware, phishing en malware.

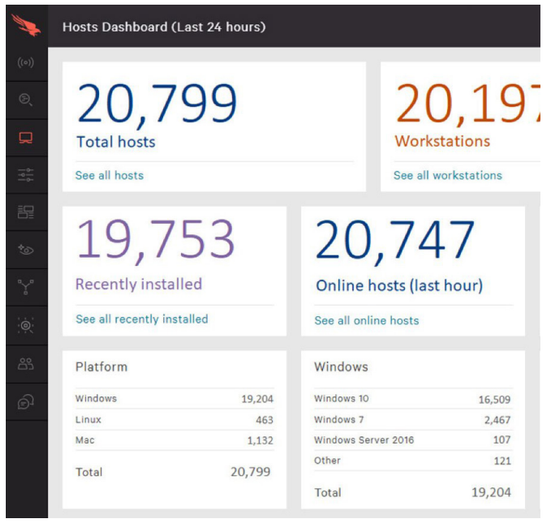
Deze complete beveiligingsoplossing detecteert niet alleen aanvallen, maar gaat ook direct en geautomatiseerd aan de slag om deze cyberaanvallen af te slaan en op te lossen. Dit gaat veel verder dan de standaard antivirus oplossingen die alleen checken op kwetsbare bestanden. De device security die wij aanbieden, kijkt ook naar aanpassingen die een bestand uitvoert op een machine door middel van 'behavior analysis'.

Device security: wat biedt de complete beveiligingsoplossing?

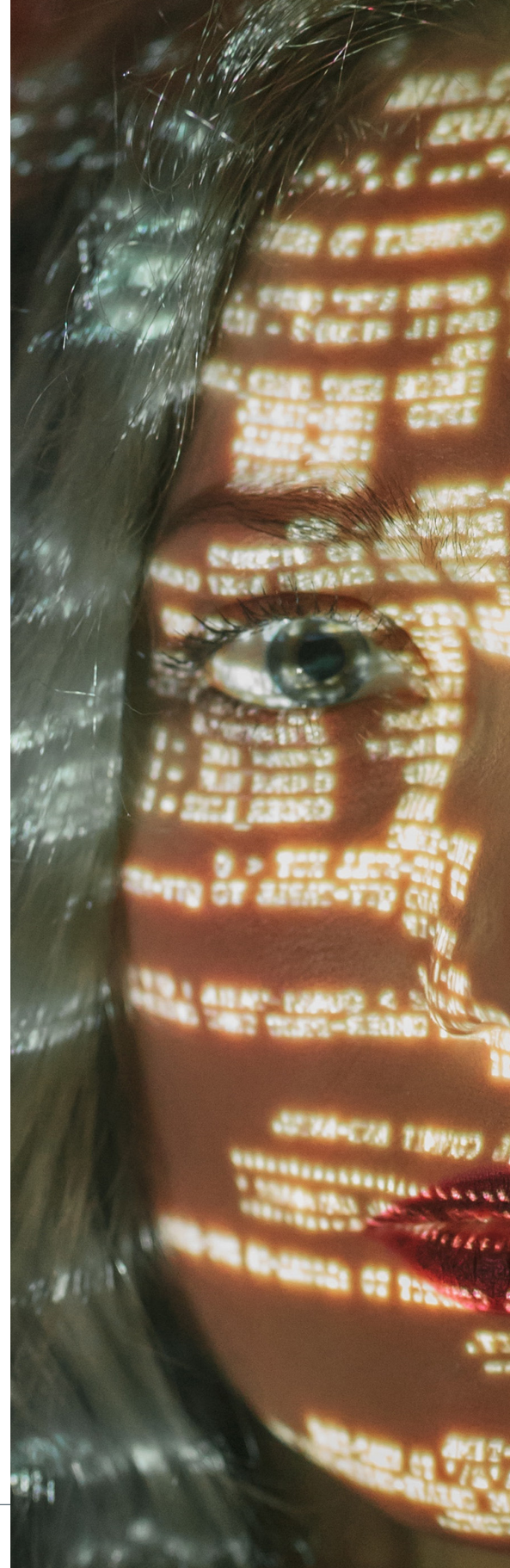
- **Next Gen Anti Virus (NGAV)**
  NGAV elimineert de tekortkomingen van de traditonele anti-virus oplossingen door anders te werk te gaan. NGAV controleert systemen op veel meer onderdelen en maakt gebruik van machine learning en artificial intelligence. NGAV kijkt onder andre naar het 'gedrag' van systemen en kan hierdoor reageren op zowel bekende als onbekende aanvallen.

- **Endpoint Detection and Response (EDR)**
  EDR geeft een compleet inzicht in de bescherming en mogelijke bedreigingen van eindpunten, en kan direct ingrijpen waar nodig. Het doel van EDR is het continu monitoren, analyseren, identificeren én voorkomen van geavanceerde aanvallen. Voordat malware daadwerkelijk wordt geïnstalleerd kan al gedetecteerd worden waar het binnen is gekomen, welk pad het bewandeld heeft op het netwerk en eindpunten en kan dus op tijd gestopt worden door EDR.

- **Security Operations Center (SOC)**
  Naast alle preventie maatregelen die we treffen met NGAV en EDR is het belangrijk om 24/7 actief bezig te zijn met het monitoren en threat hunting. Een SOC is een extern team van cyber security specialisten die niks anders doen dan kwetsbaarheden en aanvallen zoeken bij aangesloten bedrijven.



Falcon-prevent-hosts-interface



Microsoft 365 Security

Microsoft 365
geïntegreerde oplossing voor security

Op het internet is een groeiend aantal hackers en cybercriminelen actief met als doel om jouw data te stelen. Daarbij hebben zij het vooral gemunt op gevoelige informatie die, eenmaal in handen van de cybercrimineel, voor een hoop problemen kan zorgen. Dat maakt een goed beveiligde IT-omgeving tegenwoordig belangrijker dan ooit. Welke mogelijkheden biedt Microsoft 365 op het gebied van internet security?

Geïntegreerde oplossing voor security

Bij security spelen meerdere factoren een rol. Microsoft 365 biedt dan ook een geïntegreerde beveiligingsoplossing. Dankzij de integratie van Microsoft Defender voor Eindpunt, Office 365, identiteit en Microsoft Cloud App Security kunnen bedreigingssignalen compleet in kaart worden gebracht.

Zo kan worden bepaald op welke manier een bedreiging het systeem is binnengekomen, wat hiervan de impact is en welke gevolgen dit heeft voor de organisatie. Om dergelijke cyberaanvallen te voorkomen of te stoppen, onderneemt Microsoft 365 Defender automatisch actie. Hierdoor kunnen de getroffen postvakken, eindpunten en gebruikersidentiteiten worden beschermd of hersteld.

Verschillende onderdelen van Microsoft 365

Waarvoor dienen de verschillende geïntegreerde onderdelen van het Microsoft 365 pakket nu eigenlijk precies en wat kunnen zij betekenen voor jouw organisatie? We zetten de belangrijkste onderdelen op een rij:

Microsoft Defender voor Eindpunten
Dit is een beveiligingsplatform voor zakelijke eindpunten. Het helpt bedrijfsnetwerken om geavanceerde bedreigingen te voorkomen en te detecteren. Maar ook om deze (automatisch) te onderzoeken en erop te reageren. Het platform controleert continu kwetsbaarheden en verkeerde configuraties waardoor beveiligingslekken snel kunnen worden opgespoord.

Microsoft Defender voor Eindpunten maakt hierbij onder meer gebruik van sensoren die gedragssignalen van het besturingssysteem verzamelen en verwerken. Deze sensorgegevens worden geanalyseerd. De inzichten die dit oplevert dragen bij aan een effectieve bestrijding van geavanceerde bedreigingen.

Microsoft Defender voor Office 365 (e-mail).
Dit onderdeel van Microsoft 365 beschermt je organisatie tegen schadelijke bedreigingen van e-mailberichten en koppelingen (URL's). Dat gebeurt bij e-mail door een anti-phishing beleid toe te passen, maar ook door te controleren op malware, ransomware en andere aanvallen.
Koppelingen in e-mails of in bijlagen zijn voor hackers vaak aantrekkelijke plekken om een schadelijke website in te verbergen. Door koppelingen te scannen, helpt dit onderdeel van Microsoft Defender voor Office 365 je organisatie te beschermen. Het scannen van koppelingen vindt plaats naast de reguliere bescherming tegen spam en anti malware in binnenkomende e-mailberichten.

Encrypt e-mailen.
Microsoft 365 biedt daarnaast de mogelijkheid om een e-mail versleuteld te versturen. Zo kun je op een eenvoudige manier e-mails beveiligen. Bij veel overheidsinstanties, zoals gemeenten, zijn versleutelde e-mails zelfs verplicht. Encrypt e-mailen kun je vanuit Microsoft 365 naar alle andere e-maildiensten. Het is voor de ontvanger dus niet nodig om ook Microsoft 365 of Outlook te gebruiken.

Multi Factor Authenticatie (MFA)
Met het instellen van MFA voeg je een extra beveiligingslaag toe wanneer je inlogt op je Microsoft 365-account. Je aanmelden met je gebruikersnaam en wachtwoord alleen is niet veilig genoeg. Mensen hebben nogal eens de neiging om hetzelfde wachtwoord te gebruiken voor verschillende accounts of een heel voor de hand liggend woord te verzinnen dat makkelijk is te raden. Dat maakt het voor cybercriminelen wel heel gemakkelijk.

Met behulp van MFA zijn wachtwoorden minder belangrijk. Je vult namelijk niet alleen een wachtwoord in, maar ook een dynamisch gegenereerde verificatiecode die naar je mobiele telefoon is gestuurd of die je hebt gekregen via een authenticatie app. Het inbreken op accounts met gestolen of geraden wachtwoorden is hiermee verleden tijd.

Azure AD-identiteitsbeveiliging (IAM)
Het beveiligen van identiteiten is tegenwoordig een essentieel onderdeel van cyberbeveiliging voor je organisatie. IAM gebruikt hiervoor Active Directory-signalen zodat het geavanceerde bedreigingen, gecompromitteerde identiteiten en kwaadaardige acties kan ontdekken, herkennen en onderzoeken.

Door middel van geautomatiseerd identiteitsbeheer kun je de toegang tot apps en gegevens voor alle gebruikers en beheerders op efficiënte wijze controleren. Zo weet je zeker dat alleen bevoegde gebruikers toegang hebben.
Azure AD biedt gebruikers een veilige en makkelijke inlogmethode om toegang te krijgen tot hun applicaties en data. Eén Microsoft account is voldoende om overal in te loggen. Zo voorkom je een wildgroei aan accounts waarbij gebruikers vaak dezelfde, makkelijk te raden, wachtwoorden gebruiken.

Microsoft Cloud App beveiliging
Met deze uitgebreide SaaS (software as a service) oplossing heb je veel meer controle op je cloudomgeving en kun je cyberbedreigingen identificeren en bestrijden in al je cloudservices. De webapplicaties die jouw organisatie gebruikt worden toegevoegd aan een webpagina zodat je van hieruit elke applicatie kunt starten.

Back-up
Naast alle voorzorgsmaatregelen die je neemt om je IT-omgeving te beveiligen, is het natuurlijk ook altijd vereist om te beschikken over een goede back-up voor het geval er toch iets misgaat. DesktopToWork biedt een back-up oplossing waarbij er iedere dag een back-up wordt gemaakt van e-mail, OneDrive, SharePoint en Teams. Deze back-ups worden 1 jaar bewaard.

Education and Awareness

Verhoog je cyberveiligheid met trainingen Security Awareness

Jouw bedrijf heeft geïnvesteerd in cybersecurity. Met de veiligheid zit het dus wel goed, zou je denken. Maar geldt dat ook voor het personeel? Wat weten zij van cybersecurity? Herkennen zij bijvoorbeeld phishing & social engineering? Veilig omgaan met je werkplek is erg belangrijk. Daarom is het van groot belang dat iedereen binnen jouw organisatie op de hoogte is van het reilen en zeilen van cybersecurity. DesktoptoWork biedt hiervoor diverse trainingen gericht op security awareness aan.

Kasteelmuur van de 21e eeuw

Ooit ommuurden koningen hun kastelen om zichzelf te beschermen. Het hield de vijand op afstand en gold als een eerste verdedigingslinie wanneer er onverhoopt een aanval plaatsvond. Cybersecurity is de kasteelmuur van de 21e eeuw. Het biedt volop bescherming tegen mogelijke aanvallen van cybercriminelen. Het is overduidelijk dat technologie vandaag de dag essentieel is als eerste verdedigingslinie. Geavanceerde eindpuntbeveiliging, detectie van bedreigingen, SIEM-oplossingen en hulpprogramma's voor het filteren van e-mail zijn onmisbaar voor ondernemingen.

De menselijke factor

Toch kan een dergelijke verdedigingslinie pas echt optimaal functioneren als ook aan de menselijke factor is gedacht. Je moet tenslotte wel weten hoe je de verdedigingslinie het beste kunt gebruiken en hoe je de vijand kunt herkennen en verslaan. Medewerkers zijn daarom net zo goed een belangrijk onderdeel van jouw verdedigingslinie. Zelfs als je aan alles hebt gedacht en de beste technologie tot je beschikking hebt, kunnen aanvallen zoals phishing e-mails of ransomware er toch doorheen glippen. Op dat moment moet je op jouw medewerkers kunnen vertrouwen en ervan op aan kunnen dat ze een poging tot social engineering kunnen identificeren en jouw team hiervan op de hoogte kunnen stellen. Daarvoor is een training een must.

Steeds meer organisaties realiseren zich dat deze 'menselijke firewall' een belangrijke rol speelt. Cyberaanvallen richten zich vaker op werknemers. Daarom is het absoluut noodzakelijk om ook de menselijke factor te benadrukken. Je hebt meer nodig dan alleen de verschillende beveiligingssystemen. Meer dan ooit moet ook het personeel zich wapenen tegen social engineering attacks. Je ziet dan ook wereldwijd dat de menselijke firewall massaal wordt ingezet in cyberbeveiliging.

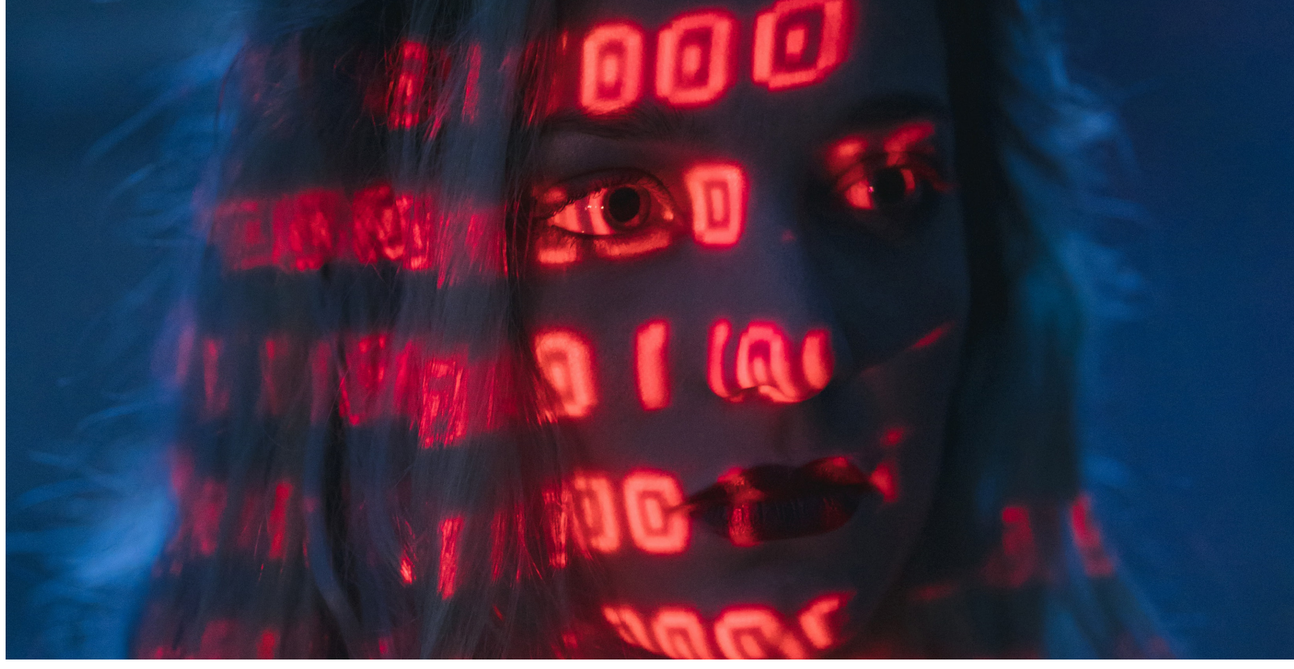
Wat is een menselijke firewall?

Een menselijke firewall bestaat uit een groep medewerkers die jouw verdedigingswerk ondersteunen door actief te letten op verdachte online- en e-mailbedreigingen. Ze melden alles wat ze gevaarlijk vinden. Hoe meer medewerkers je aan boord hebt, hoe sterker de menselijke firewall kan worden.

De meeste datalekken beginnen vaak met een fout van een werknemer. Daarom is het belangrijk dat zij er zich van bewust worden dat je het verschil kunt maken door verdachte activiteiten direct aan het beveiligingsteam te melden. Fouten kunnen op elk moment optreden, vooral omdat aanvalsvectoren complex en geavanceerd kunnen zijn, maar met een training die mensen leert om alle verdachte activiteiten te rapporteren, kun je de risico's van een succesvolle aanval minimaliseren.

Biedt de menselijke firewall 100% bescherming?

Honderd procent bescherming bieden, is een onmogelijke opgave. Fouten worden nu eenmaal altijd wel eens gemaakt, hoe goed je medewerkers ook zijn opgeleid. Dat neemt niet weg dat het veel vaker wel goed gaat, vooral als iedere medewerker zich gaat toeleggen op rapportage. In een bedrijfscultuur waarin iedereen verantwoordelijk is voor het afweren van aanvallen, maak je het werk van aanvallers een stuk lastiger.



Trainingen om jouw cyberrisico te verminderen

Met behulp van trainingen creëer je een leger van bewuste medewerkers en een succesvolle verdedigingslinie. Je medewerkers fungeren als uitkijkpost en weten dat zij mogelijke bedreigingen direct moeten rapporteren i.p.v. op verdachte links te klikken, bijlagen te downloaden of te reageren op mogelijk door criminele verzonden e-mails. Op die manier kun je inschatten of er daadwerkelijk sprake is van een bedreiging. Als dat het geval is, kan jouw team de juiste maatregelen nemen om een mogelijke aanval die waarschijnlijk meer dan één gebruiker in jouw bedrijf zou hebben bereikt, in te dammen of te beperken.

Het nut van de training Security Awareness

Je krijgt meer inzicht in aanvallen

Wanneer medewerkers e-mails gaan melden die ze verdacht vinden, krijg je veel gegevens in handen. Met geautomatiseerde oplossingen op basis van kunstmatige intelligentie en machine learning kan je de oplossingen filteren die jouw onmiddellijke aandacht nodig hebben.

Je verbetert jouw verdedigingsstrategie

Dankzij alle inzichten die je verzamelt, kun je bepalen wat het risicoprofiel van jouw organisatie is en weet je beter waar je een nog veiligere omgeving kunt creëren.

Simulatie

Een simulatie kan bijvoorbeeld een phishing mail zijn, maar kunnen ook bestaan uit andere vormen van cybercriminaliteit. Hiermee kunnen we aantonen of jouw medewerkers op dat moment voldoende bekwaam zijn geweest op basis van hun reactie.

Prestaties meten

Daarnaast kun je de prestaties van jouw organisatie meten en zien hoe deze zich in de loop van de tijd hebben ontwikkeld.

Abonnement op trainingen security awareness

DesktoptoWork biedt meerdere trainingen security awareness aan waarin we jullie medewerkers zo goed mogelijk begeleiden op dit gebied.

Enkele voorbeelden van aangeboden trainingen zijn:

- Introductie security awareness
- Hoe herken je phising & social engineering
- Veilig omgaan met mijn werkplek
- Privacy

Cyberverzekering

Een Cyberverzekering is prima aanvulling op beveiliging

Vraag jij je wel eens af of een cyberverzekering afsluiten wel nodig is? Dan leggen we je in dit artikel uit waarom het verstandig is om dit toch maar wel te doen. Je kunt voor hoge kosten komen te staan wanneer jouw organisatie niet beschikt over een adequate cyberverzekering.

100% veilige IT-omgeving bestaat niet

Wanneer je bedrijf flink heeft geïnvesteerd in een veilige IT-omgeving en het personeel daarnaast ook trainingen heeft gevolgd waardoor zij zich beter bewust zijn van de bedreigingen van cybercriminaliteit, zou je toch mogen hopen dat je voldoende bent beschermd. Uiteraard is dat ook de bedoeling en het is dan ook een verstandig besluit geweest dat je die investeringen hebt gedaan. Je hebt namelijk een belangrijke stap gezet om geen slachtoffer te worden van het groeiend aantal cybercriminelen dat op het internet actief is. Maar ondanks dat we hard ons best doen, bestaat er helaas niet zoiets als een 100% veilige IT-omgeving.

Financiële- en imagoschade

Cybercriminaliteit is aan de orde van de dag. Zo blijkt uit internationaal onderzoek dat 68% van de Nederlandse bedrijven in 2019 slachtoffer was van cybercrime. Of het nu gaat om een kassa die werd gehackt, gegevens uit je klantenbestand die op straat komen te liggen of andere gevoelige informatie waarmee de cybercrimineel aan de haal gaat, het heeft niet alleen financiële gevolgen voor je bedrijf, maar ook voor je imago.

Daarnaast geeft een cyberaanval een hoop rompslomp. Als je bijvoorbeeld te maken hebt met een datalek waarbij persoonsgegevens zijn buitgemaakt, dan ben je verplicht om dit binnen 72 uur te melden bij de Autoriteit Persoonsgegevens. Bovendien kun je een boete krijgen als je geen of te weinig maatregelen hebt genomen om een datalek te voorkomen.

Indicatie van de financiële consequenties

Wist je dat de maximale boete van de Autoriteit Persoonsgegevens maar liefst €820.000 bedraagt? Dat had je beter kunnen investeren in een robuuste cyberbeveiliging. Andere kosten waar je mee te maken kunt krijgen zijn:

- **Herstelwerkzaamheden na afloop: € 7.000**
- **Juridisch expert voor hulp bij aangifte: € 240 per uur**
- **Forensisch onderzoek naar het incident: € 4.000 per dag**
- **Kosten van gestolen of verloren data: € 185 per bestand**
- **ICT-expert om lek te repareren: € 125 per uur**
- **PR-specialist voor damage control communicatie: € 100 per uur**

Cybersecurity verzekering is een prima aanvulling
Investeren in cyberbeveiliging is dus een absolute must. Een cybersecurity verzekering vormt daarop een prima aanvulling. Om een dergelijke verzekering te kunnen afsluiten, moet je sowieso al voldoen aan een aantal voorwaarden met betrekking tot de digitale veiligheid van jouw bedrijf / organisatie.

Verzekeringsmaatschappijen willen weten hoe goed of slecht jouw cyberbeveiliging is. Je zult daarom de veiligheidsrisico's in kaart moeten brengen. Beschik je bijvoorbeeld over een goede firewall? goede antivirus software? Wordt die automatisch bijgewerkt? Maak je regelmatig back-ups? Werk je in de cloud?

Cyberverzekering via DesktopToWork

Er zijn verschillende verzekeraars op de markt, maar waarom zou je een aparte cyberverzekering afsluiten als je dit ook via ons kunt doen? Je weet dan ook zeker dat je aan alle verzekeringsvoorwaarden voldoet. Samen met onze partner in verzekeringen biedt DesktopToWork een uitgebreide cybersecurity verzekering aan.

Deze verzekering is het slot op de deur van jouw verdedigingslinie. Niet alleen ben je verzekerd tegen de financiële gevolgen van een cyberaanval en kun je aanspraak maken op schadevergoeding, je krijgt ook hulp van professionals. Met deze verzekering worden o.a. onderstaande zaken gedekt:

- **Door derden geleden schade**
- **Verdedigings- en verweerkosten voor de aansprakelijkheid bij tekortkoming van goed beheer van privacy data en andere digitale risico's**
- **Verdedigings- en verweerkosten voor de aansprakelijkheid bij tekortkoming van goed beheer van privacy data en andere digitale risico's**
- **Onderzoekskosten**
- **Kosten voor consultancy public relations ter bescherming van het imago**
- **Klant notificatie kosten**
- **Kredietbewakingskosten**
- **Boetes die door de overheid worden opgelegd (mits toegestaan)**
- **Reconstructiekosten van data**
- **Cyber afpersing**
- **Bedrijfsstilstand als gevolg van digitale risico's**

DesktopToWork

DesktopToWork helpt jou aan optimale cyberveiligheid

Een robuuste aanpak tegen cyberbeveiliging van je digitale omgeving is tegenwoordig pure noodzaak. Cybercriminaliteit is aan de orde van de dag. De dieven op het internet zijn continu op zoek naar waardevolle informatie waarmee ze je kunnen afpersen of geld afhandig kunnen maken. DesktopToWork is een expert op het gebied van cyberbeveiliging. Wij leveren echter niet alleen de beste beveiligingsproducten, maar voegen daar ook gedreven cyber experts aan toe. Door onze expertise met jouw bedrijf te delen, ontnemen we je een hoop zorgen. Op die manier kun jij je volledig richten op je *core business*.

Kwetsbare digitale infrastructuur

De Coronacrisis maakte duidelijk hoe belangrijk de digitale infrastructuur is in Nederland, maar ook dat er veel organisaties niet goed beschermd zijn tegen cybercriminelen. Het aantal cyberincidenten groeit in rap tempo. Phishing, datalekken en ransomware vormen een reëel probleem. Het Cybersecuritybeeld van de Nationaal Coördinator terrorismebestrijding en Veiligheid (NCTV) schetst dan ook een weinig optimistisch beeld over de werkelijkheid. Hoewel de pandemie de digitalisering in het bedrijfsleven, het onderwijs en de gezondheidszorg heeft versneld, wijst het jaarlijkse rapport op het gevaar dat bij onvoldoende bescherming het niet onmogelijk is dat zelfs het hele land plat kan komen te liggen.

Veilige haven in barre tijden

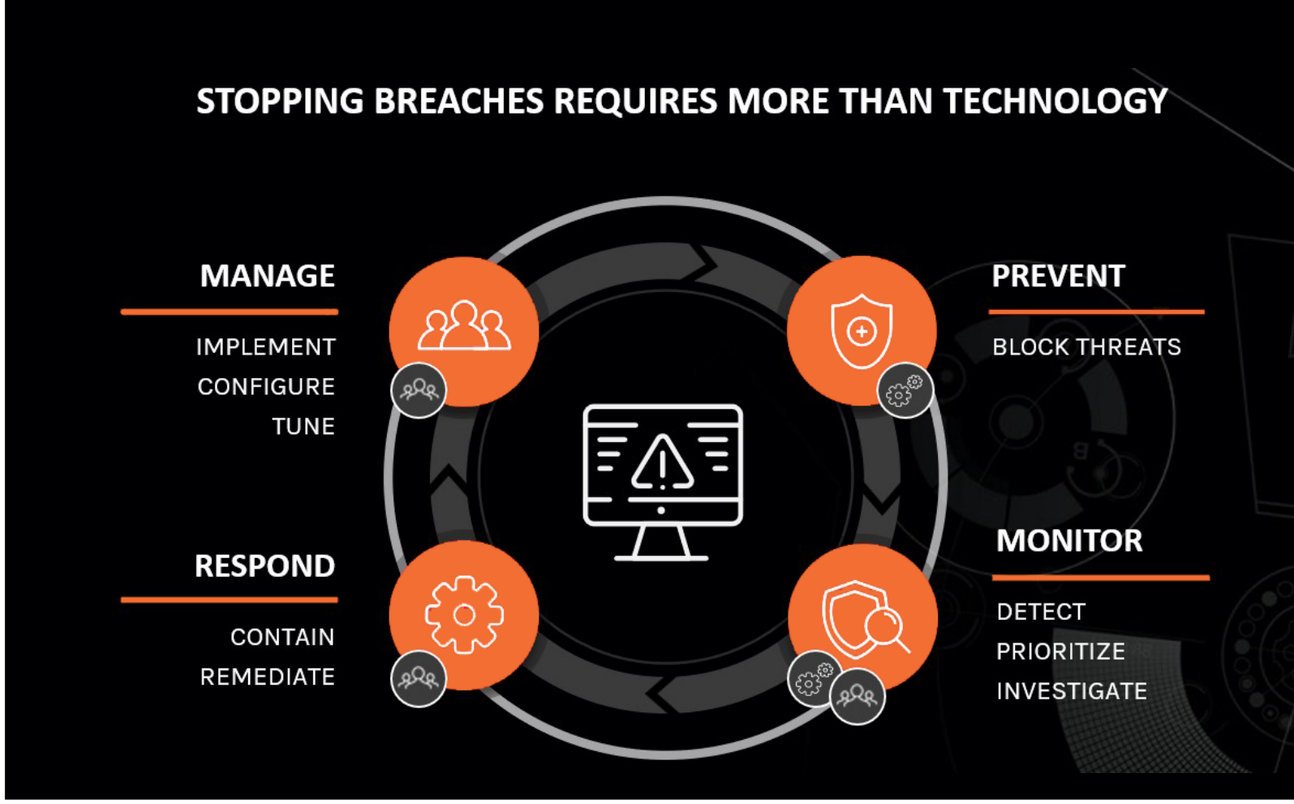
Het Cybersecuritybeeld mag dan niet al te optimistisch zijn, DesktopToWork biedt een veilige haven in barre tijden. Wij geloven dat ICT in een continue veranderende wereld veiliger moet en kan. Wij vinden dat ICT systemen bedoeld moeten zijn om ondernemers en medewerkers te ontzorgen. Zo kan iedereen binnen de organisatie zich volledig focussen op zijn eigen werkzaamheden. We zien tijd-, plaats- en apparaat onafhankelijk werken ook als een uitgelezen manier om productiever en gelukkiger te zijn. Dit alles is alleen mogelijk in een op-en-top beveiligde IT-omgeving en wanneer experts jouw bedrijfsnetwerk dagelijks controleren en updaten.

Kiezen voor de beste beveiliging

Als ondernemer ben je tegenwoordig meer dan ooit op zoek naar manieren om zo veilig mogelijk zaken te kunnen doen. Het zakelijk verkeer verloopt tenslotte steeds vaker via het internet. Je wilt daarom de beste beveiliging voor jouw bedrijf. Nu is er op het gebied van cyberbeveiliging veel beschikbaar. De vraag is echter, hoe weet je wat wel en wat niet werkt voor jouw organisatie? En als je de juiste beveiligingstools hebt aangeschaft, weet je dan ook hoe je daar optimaal gebruik van kunt maken en hoe je het moet onderhouden en bijwerken?

DesktopToWork Security, wel zo makkelijk

Hier komen onze cybersecurity-experts uitstekend van pas. Wij zorgen ervoor dat jij nauwelijks omkijken hebt naar alles wat met cyberbeveiliging te maken heeft. Wij monitoren alle systemen 24 uur per dag, zeven dagen per week en 365 daqen per jaar. Bovendien kunnen we je helpen met het up-to-date houden van alle systemen en (software) componenten binnen jouw ICT infrastructuur. Wij voegen de verschillende security onderdelen samen tot één dienst. Zo heb je alles overzichtelijk bij elkaar en blijf je volledig op de hoogte van het reilen en zeilen van jouw beveiligde omgeving.



Vulnerability scan

Zoals de naam al doet vermoeden, testen we met een geautomatiseerde vulnerability scan de kwetsbaarheden binnen jouw bedrijf. We inventariseren hoe (een onderdeel van) de IT-infrastructuur in elkaar zit en welke doelwitten – binnen de context van jouw organisatie – mogelijk interessant zijn voor hackers. Denk hierbij aan servers, systemen en laptops. Waar bevinden zich de zwakke schakels? Wat zijn voor aanvallers potentiële mogelijkheden om binnen te komen en schade aan te richten?
Daarnaast brengen we ook het niveau van het aantal updates in kaart met betrekking tot de meest uiteenlopende componenten en systemen. In de basis zijn dit uiteraard alle servers en de clients. Denk hierbij echter ook aan middle-ware software die wordt gebruikt op applicatie-servers of het patchniveau van (internet-facing) webservers.

Overzichtelijk dashboard

We houden je ook continu op de hoogte hoe het met de veiligheid van jouw netwerk en systemen is gesteld. Hiervoor gebruiken we verschillende dashboards waarop 24/7 een overzicht te zien is van alle security onderdelen binnen DesktopToWork Security. Ook kunnen er periodiek rapportages worden gemaakt en gedeeld. De security experts van DesktopToWork interpreteren de bevindingen en prioriteren de meest kritieke kwetsbaarheden. Dit alles is terug te vinden in een uitgebreid rapport. Daarin lees je welke systemen of servers het meest gevaar lopen. En waarom. Lopen ze risico om beschadigd of ontoegankelijk te raken? Of liggen er datalekken met belangrijke persoonsgegevens op de loer?

Risico's bespreken

Onze DesktopToWork Security oplossing zou echter niet compleet zijn, als hier niet ook geplande security meetings onderdeel van uit zouden maken. Tijdens deze meetings bespreken we samen met jou de stand van zaken. We bekijken welke onderdelen eventueel nog risico's kunnen lopen en waar we nog verbeteringen in de cyberveiligheid kunnen toepassen. Dergelijke meetings zijn waardevol en zorgen ervoor dat je altijd optimaal beschermd bent tegen cyberaanvallen.

Wil jij voorop lopen op het gebied van cyberveiligheid en met een gerust hart gebruik kunnen maken van al jouw systemen? Kies dan voor DesktopToWork Security. Een abonnement op veiligheid.

Security starts with Awareness

DesktopToWork Security

DESKTOP TO WORK

DESKTOP TO WORK

Contact?

085-7605000
info@desktoptowork.com
www.desktoptowork.com

Laan van Waalhaven 277
2497 GL Den Haag

Wanneer?
Op werkdagen van 07:00 – 18:00