


Leren uit COVID-19: beveiliging en continuïteitsplanning

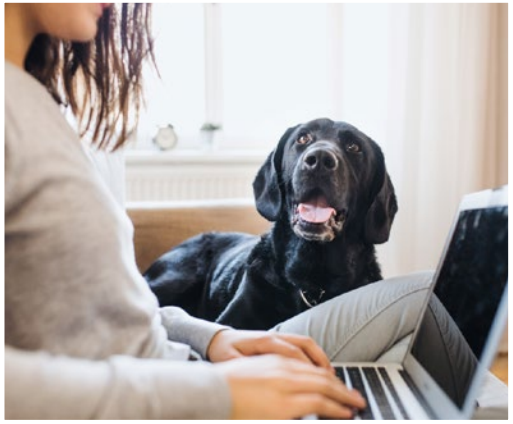
WatchGuard®

Inhoudsopgave

INLEIDING

De samenleving kampt met een pandemie: het coronavirus (COVID-19) houdt zo goed als de hele wereldbevolking in zijn greep. De scholen zijn gesloten, reizen kan niet meer onbeperkt, evenementen worden afgelast en veel kantoren liggen er verlaten bij ... We doen alles wat we kunnen om de verspreiding van COVID-19 in te perken. Het Europees Centrum voor ziektepreventie en -bestrijding heeft werkgevers zelfs aangeraden om hun werknemers thuis te laten werken, zodat ze zich gemakkelijker aan de social-distancingregels kunnen houden. Heel wat bedrijven zijn meteen in actie geschoten. Als resultaat zijn er vandaag meer telewerkers dan we ooit in de moderne geschiedenis hebben gezien. Kun je moeilijk inschatten hoe groot die impact werkelijk is? Wel, volgens een onderzoek is het aantal telewerkers in de VS tussen 2005 en 2017 met 159% gestegen. We kunnen met vrij veel zekerheid zeggen dat dit cijfer door de coronacrisis nu nog veel hoger ligt.

Door de ongeziene verandering die de coronacrisis heeft veroorzaakt, begeven veel bedrijven zich met hun nieuwe thuiswerkbeleid op onbekend terrein. In dit e-book stippelen we enkele strategieën uit om de bedrijfscontinuïteit te verzekeren, ook tijdens de coronapandemie.



LANDSCHAPSANALYSE COVID-19:
NIEUWE UITDAGINGEN OP HET VLAK VAN BEDRIJFSCONTINUÏTEIT

Elke dag krijgen we te maken met risico's op het gebied van cybersecurity. En een van de grootste uitdagingen voor wie telewerk in het hele bedrijf invoert, is dat het risico op cyberaanvallen veel groter wordt. Je gebruikers worden namelijk niet beschermd door de standaardbeveiliging van je netwerk. Ze kunnen dus ongemerkt geïnfecteerd raken en die infectie zelfs in je ruimere netwerk verspreiden zodra ze weer verbinding maken met je IT-systeem.

Hackers buiten corona-angst uit

Het lijkt wel alsof hackers van elk belangrijk nieuwsbericht en elke wereldwijde crisis gebruikmaken om hun doelwitten aan te vallen. Nu de angst regeert, worden de e-mailadressen en social media van je werknemers bestookt met nieuwsberichten, commentaren, filmpjes en links over het virus. Helaas weten cybercriminelen maar al te goed hoe ze deze angst kunnen misbruiken om je gebruikers te phishen, te hacken of malware op hun systeem te zetten.

Hieronder sommen we slechts enkele voorbeelden op van hoe aanvallers de coronacrisis uitbuiten:

- **Doen alsof ze de Wereldgezondheidsorganisatie (WHO) zijn.** TDe WHO heeft gemeld dat er verdachte phishingberichten worden verstuurd door mensen die zich voordoen als de organisatie. Die berichten bevatten zogezegd levensbelangrijke gezondheidsinformatie. Om die 'informatie' te krijgen, moeten slachtoffers op een link klikken, een bestand downloaden of gevoelige informatie doorgeven.

- **Malware installeren**. AEen groep hackers heeft van de coronapandemie gebruikgemaakt om slachtoffers in Mongolië te infecteren met een tot nu toe onbekende soort malware. Hun offensief, genaamd 'Vicious Panda', is nog maar net aan het licht gekomen.

- **De Emotet-trojan spammen**. Hackers hebben Japanse gebruikers bestookt met op het eerste gezicht nuttige meldingen over hoe je de verspreiding van het coronavirus kunt tegengaan. Met die spamcampagne wilden ze de Emotet-trojan verspreiden. Emotet is in staat om e-mailaccounts te hacken, berichten te spoofen en zo dieper in een IT-systeem binnen te dringen.

- **Ransomware installeren via een valse app voor virustracering.** Een app die eruitziet als een landkaart die corona-uitbraken weergeeft, is eigenlijk ransomware die je telefoon vergrendelt. De app, 'COVID19 Tracker', infecteert je apparaat en eist $ 100 in bitcoin als 'losgeld' binnen 48 uur.

Uit het beveiligde netwerk geplukt

Door COVID-19 hebben veel bedrijven een doorgedreven thuiswerkbeleid ingevoerd: bijna van de ene dag op de andere gingen de kantoren op slot en moesten de meeste werknemers thuis aan de slag. Hoewel werkplekflexibiliteit nu in tal van ondernemingen de norm is, werkt normaal gezien slechts zo'n 30 % van het personeel van een gemiddeld bedrijf van thuis uit. Veel bedrijven hebben niet de middelen om iedereen veilig te laten telewerken. Werknemers kregen snel een laptop toegestuurd of moesten zelfs hun desktop-pc meenemen, terwijl het net niet de bedoeling is om deze computers uit het beveiligde bedrijfsnetwerk te halen. Nu deze apparaten uit het netwerk geplukt zijn, hebben ze niet alleen extra beveiliging nodig. Minstens even belangrijk is dat ze geen malware en andere bedreigingen je systemen binnenloodsen zodra ze weer verbinding maken met je netwerk – via VPN of wanneer je werknemers terugkeren op kantoor.

Overbelaste VPN's

Nu talloze werknemers door de coronacrisis van thuis uit werken, is het internetverkeer via VPN's enorm gestegen: onderzoekers zagen een toename van 50% in één week tijd. Alleen al in de Verenigde Staten zal het VPN-gebruik in één maand tijd naar verwachting met 150% stijgen. Door de plotse overgang van bedrijfs- naar thuiskantoren zitten veel ondernemingen met de handen in het haar, want al die telewerkers hebben zo snel mogelijk een VPN-licentie nodig. Zonder VPN-verbinding bestaat namelijk het risico dat de werknemers geen toegang krijgen tot het materiaal dat ze nodig hebben, of moeten ze dat materiaal te pakken krijgen via een onveilige verbinding.

Bandbreedte bezet

Niet alleen je werknemers zijn thuis. Nu de scholen gesloten zijn, moeten de kinderen van veel collega's hun lessen online volgen. Hebben ze geen les, dan gamen ze misschien of surfen ze gewoon op het web. En als iedereen het internet nodig heeft, wordt het moeilijk om al dat verkeer te slikken. Dat geldt zeker als er toepassingen worden gebruikt die veel bandbreedte vereisen, zoals videoconferenties. In de regio's waar het virus het ergst om zich heen grijpt, is het internetgebruik met meer dan 90 % gestegen. Als reactie upgraden veel internetproviders de bandbreedte van hun klanten naar een snellere, betere versie of schaffen ze datalimieten af. Zo moeten gezinnen niet vrezen dat ze hun limiet zullen overschrijden.

Het VPN-gebruik is de hoogte in geschoten: **in één week tijd steeg het verkeer met 50%.**

Alleen al in de Verenigde Staten zal het VPN-gebruik met 150% stijgen in één maand tijd.

ACHT TIPS VOOR IT-LEIDERS: BEVEILIGING ALS SLEUTEL VOOR PRODUCTIVITEIT EN TOEGANG

1. INVENTARISEER EN EVALUEER DE THUISWERKMIDDELEN VAN JE BEDRIJF

92 % van alle ondernemingen laten hun werknemers thuiswerken, maar niet iedereen krijgt hierbij dezelfde kansen. Veel bedrijven moesten bijna van de ene op de andere dag overstappen naar telewerk en hadden dus niet genoeg tijd om alles goed te plannen. Dit is het ideale moment om de nieuwe netwerktoegang die je bedrijf nodig heeft te evalueren en te beoordelen, en om de gevolgen op beveiligingsvlak te onderzoeken. Managed Security Services Providers (MSSP's) zijn experts in beveiligingsaudits die middelgrote ondernemingen kunnen helpen om hun systeem snel up-to-date te krijgen, zodat ze hun gebruikers kunnen bieden wat ze nodig hebben.

Netwerknomaden die altijd onderweg zijn, beschikken waarschijnlijk al over geschikt materiaal om de komende tijd te kunnen verder werken. Maar voor de medewerkers die niet vaak thuiswerken, is het nuttig om een inventaris op te stellen met alle gegevens en toepassingen die ze vaak gebruiken. Op basis hiervan kun je uitstippelen wie toegang nodig heeft tot welke bestanden en software – en hoe je die toegang het best organiseert. Werk samen met de afdelingshoofden om de unieke behoeften van elk team in kaart te brengen, zodat de teamleden ook thuis het beste van zichzelf kunnen geven.

Hou rekening met de punten in deze checklist:

- ✔ Heeft de werknemer een bedrijfsapparaat of moet je extra gsm's/laptops voorzien?
- ✔ Heb je genoeg VPN-licenties voor iedereen of heb je extra licenties nodig?
- ✔ Volstaat de internetverbinding van de werknemer om zijn of haar taken naar behoren te kunnen uitvoeren?
- ✔ Welke systemen heeft de werknemer nodig om zijn of haar taken uit te voeren?
- ✔ Heeft de werknemer beveiligde toegang tot gevoelige systemen en gegevens nodig?
- ✔ Welke cloudtoepassingen gebruikt de werknemer regelmatig?
- ✔ Kan de werknemer multi-factorauthenticatie gebruiken?

2. BEPAAL DE VERWACHTINGEN VOOR TELEWERK EN COMMUNICEER EROVER

Veel werknemers werken nu voor het eerst van thuis uit. Dit is dus het ideale moment om het telewerkbeleid van je bedrijf aan je team mee te delen en de thuiswerkers te laten weten wat er van hen wordt verwacht. Ongeveer 24 % van alle ondernemingen heeft een thuiswerkbeleid dat al meer dan een jaar niet meer aangepast is. Grijp dus je kans om dit nu te doen. Met een eenvoudige e-mail of conference call met je team bereik je al veel.

Enkele punten om te vermelden:

- **Beschikbaarheid** - Welke werkuren verwacht je van je team? Wanneer ben je zelf bereikbaar?
- **Reactietijd** - Moeten telewerkers onmiddellijk reageren? Zo ja, hoe gaat dit in zijn werk? Bijvoorbeeld: worden écht dringende vragen alleen telefonisch gesteld?
- **Platformen** - Herinner je werknemers eraan welke tools en platformen ze moeten gebruiken: cloudopslagplatformen, communicatie- en videoconferentietools, projectbeheertools enz. Druk je teamleden op het hart dat ze geen niet-goedgekeurde platformen mogen gebruiken.
- **Apparaten** - Wijs je teamleden op het gebruiksbeleid van de apparaten die ze van het bedrijf hebben gekregen. Gebruiken ze persoonlijke apparaten voor hun taken? Dan is dit het juiste moment om samen met hen te bekijken welke apparaten geschikt zijn en welke regels ze moeten volgen als ze via hun eigen apparaat willen werken.
- **Incidenten melden** - Waar kunnen werknemers terecht als ze vermoeden dat bedrijfsgegevens in gevaar zijn? Aan wie moeten ze het datalek melden en welke stappen moeten ze ondernemen om de schade te beperken?

3. CYBERSECURITY ALS DEEL VAN DE BEDRIJFSCULTUUR

De meeste bedrijfsleiders weten dat het succes van een onderneming staat of valt met de bedrijfscultuur. Wat ze ook moeten inzien, is dat hetzelfde geldt voor cybersecurity. Wanneer je werknemers blootgesteld worden aan gerichte aanvallen (en aanvallers misschien zelfs doen alsof ze een van je teamleden zijn), kan de bedrijfscultuur het verschil maken: wordt de aanval onderschept of wordt je netwerk volledig geïnfecteerd?

Hackers gebruiken technieken om je gebruikers te manipuleren en te beïnvloeden tot ze doen wat zij willen. Autoriteit en dringendheid zijn twee van hun belangrijkste wapens. Als leidinggevende moet jij duidelijk maken dat iedereen vrijuit kan spreken: alle werknemers, van de hoogste tot de laagste functie, moeten weten dat hun melding steeds serieus zal worden genomen als ze een mogelijke bedreiging opmerken.

Tips om cybersecurity in te passen in je bedrijfscultuur:

- **Deel verhalen.** Heeft een werknemer een phishingmail onderschept of is zijn laptop geïnfecteerd door ransomware? Deel het verhaal met je andere werknemers: zo beseffen ze dat dit soort bedreigingen geen 'ver-van-mijn-bedshow' zijn en kunnen ze soortgelijke aanvallen voorkomen. Het is ook een goed idee om iedereen te vertellen over aanvallen tegen bedrijven zoals het jouwe.
- **Beloon goed gedrag.** Als een werknemer een mogelijke aanval meldt, bespaart hij je bedrijf heel wat potentiële kopzorgen. Dat verdient een beloning! Met incentives voor het melden van verdachte activiteiten stimuleer je je werknemers om alert te zijn en om erover te praten met collega's.
- **Wees aardig.** Laten we eerlijk zijn: bij de meeste bedrijven werken mensen met erg uiteenlopende technologische vaardigheden. Het is gewoon niet realistisch om te verwachten dat je werknemers elke bedreiging kunnen afweren en steeds alle richtlijnen zullen volgen. Vergissen is menselijk. Daarom is het erg belangrijk dat je begrip toont.

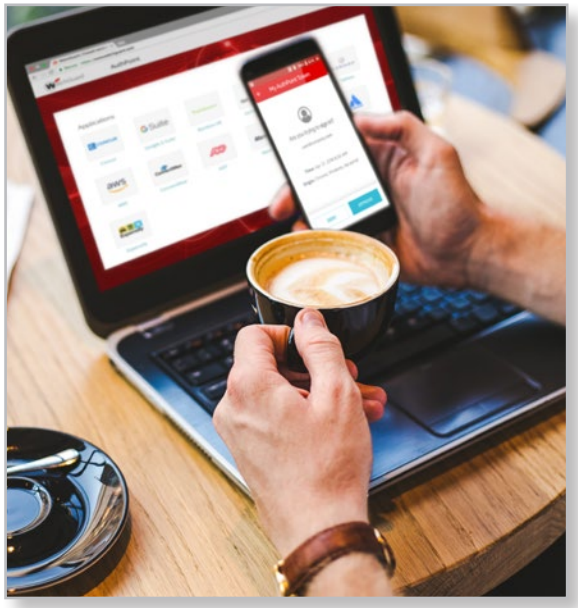
4. VOER MULTI-FACTORAUTHENTICATIE IN

Nu de meeste werknemers overstappen naar telewerk, moeten bedrijven ervoor zorgen dat iedereen veilig toegang krijgt tot de nodige interne tools. Een grote uitdaging voor veel ondernemingen. Tegelijkertijd gaan hackers steeds vaker op zoek naar aanmeldgegevens en hebben ze het dus specifiek gemunt op de accountgegevens van je gebruikers. Daarom raden we aan multi-factorauthenticatie (MFA) in te voeren voor al je gebruikers, zodat ze zich volledig moeten identificeren telkens wanneer ze verbinding maken met je netwerk.

Multi-factorauthenticatie stelt je ook in staat om de toegang tot cloudtoepassingen en -omgevingen te beveiligen als telewerkers deze rechtstreeks via het internet gebruiken. Zo voeg je een extra beschermingslaag toe, wat erg nuttig is nu veel bedrijven bijzonder kwetsbaar zijn.

Waarop moet je letten bij een MFA-oplossing?

- **Cloudgebaseerd.** Sommige MFA-oplossingen kunnen niet zonder hardwaretoken. Een cloudgebaseerd systeem werkt anders: de gebruiker installeert gewoon een app op zijn telefoon en kan dan snel en gemakkelijk aan de slag.
- **Voor alle toepassingen.** Je oplossing moet goed integreerbaar zijn, zodat deze alle belangrijke toepassingen beveiligt die je werknemers nodig hebben.
- **Eenvoudig.** De oplossing moet intuïtief aanvoelen, want niet al je gebruikers zijn even technisch vaardig.
- **Meeerdere authenticatiemethodes.** Met ondersteuning voor meerdere online en offline authenticatie-opties krijgen geautoriseerde gebruikers toegang tot wat ze nodig hebben, wanneer ze het nodig hebben.
- **Werkt met meerdere tokens.** MFA wordt tegenwoordig vaak aangeboden door social-mediawebsites, banken, handelszaken en meer. Zoek een oplossing waarmee je tokens kunt samenvoegen in één eenvoudige MFA-toepassing, zodat je gebruikers overal vlot toegang toe krijgen.



5. GEEF OOK PRIORITAIRE GEBRUIKERS TOEGANG VIA VPN

Een veilige verbinding met je hoofdkantoor en kritieke toepassingen is essentieel als je wilt dat je werknemers thuis even productief zijn als op kantoor. Met virtuele privénetwerken (VPN's) voeg je een extra beveiligingslaag toe aan openbare en privénetwerken, zodat personen en organisaties op een veilige manier gegevens via het internet kunnen verzenden.

Over het algemeen hebben je gebruikers een van de volgende twee VPN-types nodig:

1. **Clientgebaseerd VPN.** Een clientgebaseerd VPN werkt op het niveau van het netwerk en geeft gebruikers toegang tot het volledige netwerk.

2. **Clientloos VPN.** Voor clientloze VPN's heb je meestal alleen een browser nodig. Via deze VPN's maken gebruikers verbinding met specifieke toepassingen en diensten.

Meestal voorzien bedrijven slechts VPN's voor een beperkte groep telewerkers en werknemers die vaak onderweg zijn, niet voor het voltallige personeel. Nu het VPN-gebruik toeneemt, is het belangrijk dat je dit goed beheert en storingen voorkomt. Denk dus aan deze tips:

- **Geef gebruikers met een verhoogd risico prioriteit.** Sommige werknemers hebben meer nood aan een VPN dan andere, en sommige hebben helemaal geen VPN-toegang nodig. Breng dus in kaart wie toegang nodig heeft tot welke toepassingen en stel dan je VPN-verbindingen beschikbaar op basis van prioriteit. Zo raakt je netwerk nooit overbelast.

- **Gebruik een cloud-hosted firewall om steeds aan de vraag te voldoen.** De vraag naar VPN-services piekt, maar dat betekent niet dat je plaats in de serverruimte moet vrijmaken. Met een cloud-hosted firewall verlicht je de belasting van het VPN-verkeer naar je hoofdkantoor en stem je de beveiliging af op de verbindingen die je bedrijf werkelijk nodig heeft.

- **Verplicht MFA.** Zonder MFA kan een hacker die één set VPN-aanmeldgegevens te pakken krijgt, je volledige netwerk doorzoeken. Gebruikers die via een VPN verbinding maken, moeten zich dus steeds met minstens twee factoren authenticeren.

- **Gebruik een tabletop firewall.** Een tabletop firewall in het thuiskantoor van je gebruikers biedt volledige UTM-beveiliging zonder het VPN van je bedrijf te belasten.

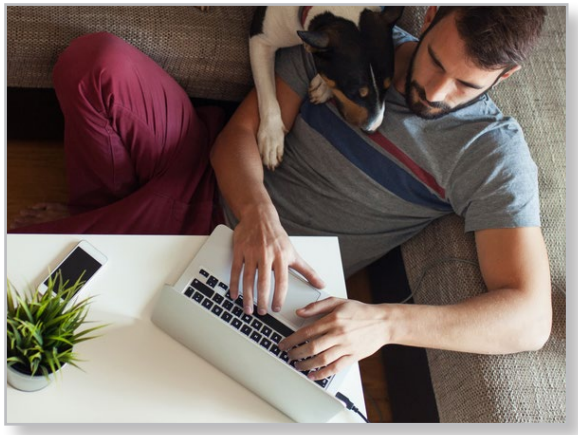
6. VOORKOM RISKANT KLIKGEDRAG MET EEN DNS-FILTER

Het is moeilijker om gebruikers online te beschermen als ze buiten je netwerk surfen. Nu heel wat werknemers thuis moeten blijven, is de kans groot dat ze hun bedrijfslaptop veel vaker zullen gebruiken in hun vrije tijd – om te surfen of hun persoonlijke mails te lezen, bijvoorbeeld. Met een cloudgebaseerde DNS-filter kun je bepaalde verbindingen blokkeren en je werknemers weghouden van de gevaarlijke uithoeken van het internet. Zo voorkom je dat mensen op een schadelijke link klikken of een domein willen openen dat gelinkt is aan phishing en malware – en je hebt er niet eens een VPN voor nodig!

Denk hieraan als je een DNS-filteroplossing kiest:

- **Handhaving van productiviteit en beleidsregels.** Nu er meer werknemers niet op kantoor werken, moet je mogelijk stappen ondernemen om hun productiviteit op peil te houden. Dit kun je bijvoorbeeld doen door de toegang tot bepaalde inhoud te beperken. Denk maar aan social media en 'pikante' websites. Zoek dus een oplossing met uitgebreide controleopties, zoals de mogelijkheid om gebruikers en groepen te blokkeren en uren in te stellen waarbinnen de beperkingen gelden.

- **Ondersteuning voor beveiligingstraining.** De meeste bedrijven laten hun werknemers een opleiding over cybersecurity volgen. Nu veel werknemers elders werken, is het belangrijker dan ooit dat ze die leerstof ook echt toepassen. Sommige DNS-filters blokkeren niet alleen schadelijke verbindingen, maar herinneren de gebruiker er ook aan hoe ze soortgelijke bedreigingen in de toekomst kunnen herkennen.



7. HOU ENDPOINTS VRIJ VAN MALWARE

Door de coronacrisis is het aantal malware- en ransomwareaanvallen alleen maar toegenomen. En het infectierisico is nog nooit zo hoog geweest, want telewerkende gebruikers worden niet beschermd door de bedrijfsfirewall. Endpoint-antivirusoplossingen kunnen tal van bedreigingen onderscheppen, maar ze staan machteloos tegen de listige zero-day malware waarmee we vaak te maken krijgen. Oplossingen voor endpointdetectie en -reactie (EDR) detecteren niet alleen deze geavanceerde bedreigingen, maar elimineren ze ook en herstellen het geïnfecteerde apparaat naar de normaal werkende toestand. En dat gebeurt allemaal 100 % op afstand.

Essentiële kenmerken van een EDR-oplossing:

- **Detectiemethodes.** Om geavanceerde malware te detecteren, heb je geavanceerde methodes nodig. Zoek een oplossing die verschillende detectiemethodes combineert, zoals gedrags-, heuristische en sandboxanalyse.

- **Automatisering en AI.** Een oplossing die snel op bedreigingen reageert, bespaart je heel wat kopzorgen. Met automatische detectie en reactie gebeurt dit zo goed als onmiddellijk.

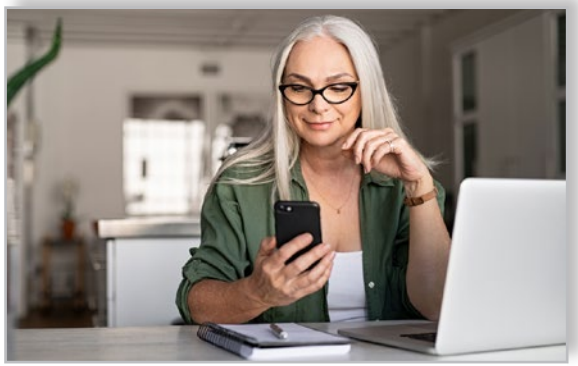
- **De host afzonderen.** Als het systeem een bedreiging opmerkt, moet dit de geïnfecteerde host meteen weg van de rest van je netwerk isoleren. Zo voorkom je dat de infectie zich verder verspreidt.

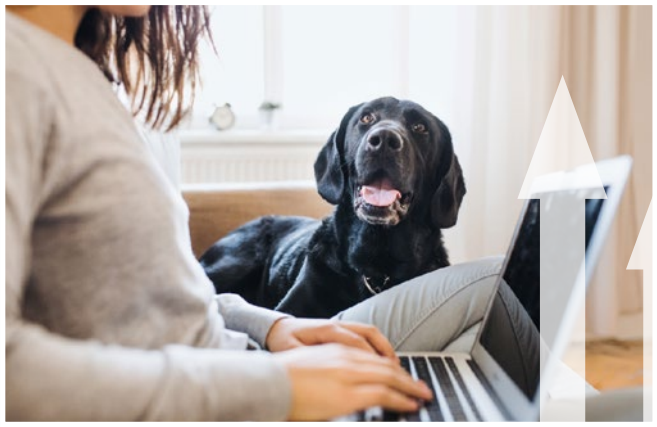
8. HOU WIFI ONDER CONTROLE

Thuiswerk kan dus ook door dat wifiverkeer beveiligingsproblemen met zich meebrengen. Bij telewerkers in een dichtbevolkte woonzone, zoals een appartementsgebouw, kan elk wifi-apparaat een deurtje openen voor kwaadwillige buren die willen meekijken of -luisteren. Zelfs een deurbel, gamingconsole of IoT-apparaat. Als zo'n kwaadwillige buur in een appartementsgebouw vol telewerkers woont en als je weet dat bijna 50 % van al het IP-verkeer via wifi verloopt, kun je je wel voorstellen hoe groot het risico is.

Denk aan het volgende voor telewerk via wifi:

- **Gebruik Trusted Wireless Environment-gecertificeerde toegangspunten**, zoals WatchGuard AP225W, om je IT-afdeling een volledig overzicht te geven van de client- en netwerkprestaties. Zo kunnen ze je telewerkers optimaal ondersteunen.
- **Configureer toegangspunten vooraf**, zodat ze gemakkelijk bij de gebruiker thuis kunnen worden geïnstalleerd.





In dichtbevolkte zones, zoals appartementsgebouwen, verloopt bijna **50% van al het IP-verkeer** via wifi.

WAAROM EEN GOED VOORBEREID BEDRIJF ER TWEE WAARD IS BIJ IT-BEVEILIGING

Kort gezegd: sommige dingen kan niemand voorspellen. Bedrijfsleiders weten dat er bij elk proces problemen en ongeplande incidenten kunnen opduiken. Hoe kun jij dan de toekomst van je bedrijf veiligstellen? Een voorbereidingsplan garandeert niet dat je perfect beschermd bent, maar het geeft je wel de tools die je nodig hebt om uitdagingen op een veilige manier te overwinnen en je operationele continuïteit te verzekeren.

Vandaag kampen we met de coronacrisis, maar morgen kan er een heel ander probleem ontstaan, en dat hoeft niet noodzakelijk een ramp te zijn. Denk maar aan een groot evenement, zoals het wereldkampioenschap voetbal, dat de normale gang van zaken in een hele stad verstoort. Zelfs een menselijke fout kan ertoe leiden dat je je kritieke voorbereidingsplan in het hele bedrijf moet activeren. Elke situatie waarin je je snel aan onverwachte veranderingen moet aanpassen, is het ultieme bewijs dat het écht belangrijk is om goed te weten hoe je organisatie in elkaar zit en welke behoeften er zijn.

Waarom? Omdat je je werknemers, klanten en stakeholders zo toont dat je bedrijf zelfs tijdens een ongeziene crisis probleemloos aan de slag blijft. Ja, dat is mooi voor je merkimago, maar nog belangrijker is dat je community je bedrijf zo door en door vertrouwt. Bovendien hou je er een erg waardevol verhaal aan over dat je nog jarenlang als troef kunt gebruiken.

Waarom? Omdat je je werknemers, klanten en stakeholders zo toont dat je bedrijf zelfs tijdens een ongeziene crisis probleemloos aan de slag blijft.

IT-CHECKLIST BEDRIJFSCONTINUÏTEIT

Evaluatie: is jouw bedrijf klaar voor thuiswerk?

Is mijn bedrijf voorbereid?	Ja	Nee	Actie
Heb je in de voorbije twaalf maanden je thuiswerkbeleid geüpdatet?			
Heb je het beleid en je verwachtingen meegedeeld aan alle werknemers die nu thuiswerken?			
Moet je extra gsm's/laptops aankopen om ervoor te zorgen dat alle werknemers over een goedgekeurd apparaat beschikken?			
Heb je genoeg VPN-licenties voor iedereen indien nodig?			
Volstaat de internetverbinding van de werknemer om zijn of haar taken naar behoren te kunnen uitvoeren?			
Heb je in kaart gebracht of telewerkers toegang hebben tot de systemen of platformen die ze nodig hebben om hun taken te kunnen uitvoeren? *bijv. cloudtoepassingen*			
Kan je bedrijf beveiligingssystemen inzetten om mogelijke cyberaanvallen bij telewerkers te voorkomen? *bijv. beveiligde wifi, VPN-verbinding, multi-factorauthenticatie*			
Moet je je IT-budget aanpassen om de nodige middelen te kunnen voorzien?			
Moet je je personeel een opleiding over veilig telewerken aanbieden?			

GRATIS DIENSTEN DIE KMO'S HELPEN TIJDENS DEZE ONGEZIENE CRISIS

Om bedrijven te helpen bij het beschermen van hun telewerkers, biedt WatchGuard zijn diensten tijdelijk gratis of met korting aan. Ga naar onze **Remote Workers Resource pagina** en ontdek er de uitzonderlijke aanbiedingen voor WatchGuard Passport. Deze bundel beveiligingsservices voor gebruikers is speciaal ontworpen om phishingpogingen te blokkeren, het internetbeleid te handhaven en mensen overal ter wereld veilig te laten inloggen.

Meer informatie

Wil je meer informatie? Praat dan met je erkende WatchGuard-verdeler of ga naar **https://www.watchguard.com.**

Over WatchGuard

WatchGuard® Technologies, Inc. is een wereldwijde marktleider op het vlak van netwerkbeveiliging, wifi-beveiliging, multi-factorauthenticatie en network intelligence. De bekroonde producten en services van het bedrijf worden wereldwijd vertrouwd door bijna 10.000 verdelers en serviceproviders en beschermen meer dan 80.000 klanten. WatchGuard heeft één missie: beveiliging op enterpriseniveau eenvoudig en toegankelijk maken voor alle bedrijven, ongeacht hoe groot of klein ze zijn en tot welke sector ze behoren. Dit maakt van WatchGuard de ideale oplossing voor middelgrote bedrijven en ondernemingen met meerdere filialen. Naast de hoofdzetel in Seattle, Washington (VS) heeft het bedrijf kantoren in heel Noord- en Latijns-Amerika, Europa en Azië/Oceanië. Meer informatie vind je op WatchGuard.com.

North America Sales: 1.800.734.9905 • International Sales: 1.206.613.0895 • Web: www.watchguard.com