



Thuiswerken is goed, veilig thuiswerken is beter

De voordelen van een zakelijke verbinding thuis

IRISONE^{ICT}



In Nederland werken we massaal thuis via digitale werkplekken. Vanwege de toegenomen cyberdreiging zijn we bezorgd dat onze gegevens gestolen worden. En dat is terecht. We lezen tenslotte dagelijks in de media dat bedrijven door cybercriminelen lam worden gelegd. Dit wil jij natuurlijk voorkomen. Dat kan met veilige werkplekken én verbindingen.

Werken jouw collega's veilig thuis?

Het [Cybersecurity onderzoek Veilig Online 2021](#) van de overheid laat zien dat Nederlanders bewuster omgaan met cybersecurity dan voorheen. Ook worden ze steeds vaker geconfronteerd met cybercriminaliteit. Nu we ons steeds meer in cyberspace ophouden, hebben [criminelen hun werkveld verlegd](#). Een derde van de Nederlandse volwassenen heeft zelf ooit weleens te maken gehad met een poging tot phishing. De frauduleuze e-mails blijven onverminderd populair én gevaarlijk. Één klik op de verkeerde link en het bedrijfsnetwerk kan zomaar in handen komen van cybercriminelen. Een ramp voor bedrijven, want wie kan zonder werken de internetverbinding en toegang tot bestanden en apps nog werken?

Gek: thuis werken we niet volgens zakelijke eisen

Werken je collega's wel echt veilig vanuit huis? Thuis stellen we meestal minder hoge eisen aan de verbinding en cybersecurity. Op ons werk eisen we een zakelijke verbinding. Eentje die het altijd moet doen, waar de bandbreedte nooit de beperkende factor mag zijn en waar de veiligheid

optimaal is dankzij 24/7 checks op gevaarlijke activiteit.

De wet eist bovendien van bedrijven dat de dataveiligheid in orde is. Desondanks blijkt uit verschillende onderzoeken dat dit in het mkb [niet altijd goed geregeld](#) is, maar is het bij thuiswerkers beter? Hier lees je oplossingen voor thuiswerken, maar dan volgens zakelijke eisen.

1 Neem een zakelijke lijn thuis

Op kantoor, maar ook voor al je thuiswerkers, wil je niet alleen een stabiele, maar vooral ook een veilige verbinding. Wil je dat medewerkers nog werken via hun eigen verbinding, of bied je ze liever ook een zakelijke lijn met de bijhorende voordelen op het gebied van stabiliteit en veiligheid? Met een zakelijke verbinding bij je medewerkers thuis bied je de best mogelijke oplossing. Via deze verbinding kunnen ze privé internetten en gaan ze voor het zakelijke gedeelte via een beveiligde verbinding aan de slag. Deze zakelijke verbinding kun je natuurlijk ook regelen voor je kantoor.

2 Zet een hek om alle gevaarlijke websites

Er is ook nog een derde manier om de verbinding te beveiligen. Dat kan met Extra Veilig Internet (EVI). Er dreigt natuurlijk nog altijd het gevaar van malafide websites. Thuiswerkende collega's klikken nog wel eens per ongeluk op een phishing-mail of bezoeken een frauduleuze site. Denk ook aan hun kinderen die misschien met de computer van pa of ma onveilige sites bezoeken. Dit brengt de dataveiligheid van het hele bedrijfsnetwerk in gevaar. En dan heb je ook nog de slimme koelkasten, internetradio's en IP-camera's waarvan de beveiliging niet altijd optimaal is.

Met EVI zet je een hek om alle gevaarlijke websites. Bevat een site malware of andere gevaarlijke content, dan zie je een waarschuwingspagina. Zo houd je cybercriminelen buiten de deur. EVI blokkeert ook verkeer naar onveilige webadressen. Dit verhindert misbruik van gekaapte laptops en blokkeert malafide verkeer naar het groeiend aantal slimme apparaten. EVI beschermt je tegen cybercrime vanaf het internet, maar het gevaar komt ook van andere kanten.

3 Beveilig alle eigen smartphones en laptops

Waarschijnlijk werken veel medewerkers met een eigen laptop of smartphone via een privé internetabonnement. Maar zijn die apparaten wel goed beveiligd? Je moet kunnen vertrouwen op een systeem dat geavanceerde bedreigingen detecteert, onderzoekt en uitschakelt. Je wil niet dat ieder zijn eigen virusscanner heeft. Beter is één systeem dat alle computers, laptops, smartphones en tablets in de gaten houdt. Want als één privé laptop geïnfecteerd raakt met een virus, lift die misschien via de volgende thuiswerksessie naar kantoor... Met Microsoft Defender for Business krijg je centraal grip op alle devices. Dus ook iPhones, Macs en Android-apparaten. Met deze integrale oplossing bescherm je alle werkplekken tegen virussen, spyware en andere schadelijke software. Bovendien kunnen alle losse virus-scanners de deur uit.

4 Installeer een goede firewall

Zonder firewall staat de poort voor iedereen open. Maar hebben je thuiswerkers wel een goede firewall? De meeste collega's hebben thuis een standaard router, zonder firewall en zonder beheer. Vraag daarom je IT-leverancier voor extra beveiliging met een firewall van zakelijke kwaliteit. Daarmee gooi jij je netwerk op slot voor onbevoegden.

5 Thuis en op kantoor altijd verbonden

Je wil een betrouwbare partner zijn voor je klanten. Dat lukt alleen als je dataveiligheid goed regelt en altijd verbonden bent. Jij kunt dit bieden door thuiswerkende medewerkers op een zakelijke manier te verbinden. Met een stabiele en goed beveiligde internettoegang garandeer je een optimale aansluiting op de 24/7-maatschappij.

Het kan wel eens voorkomen dat het internet thuis niet werkt. Een storing in de wijkcentrale of iets te enthousiaste graafwerkzaamheden kunnen zorgen voor een kink in de kabel. Downtime kost tegenwoordig geld en klanten, dus je wil een verbinding die het altijd doet. Los het op met een simkaart in je router. Valt de verbinding weg, dan schakelt de router automatisch door via het supersnelle mobiele 4G-netwerk. Hierdoor blijft je thuiswerkende collega altijd online en kan het werk doorgaan. Op die manier zorg je ook dat je kantoor altijd verbonden is met klanten én je thuiswerkende collega's. Dankzij 4G Back-up zijn ze thuis of op kantoor altijd online.

Thuiswerken is het nieuwe normaal, thuiswerken met een zakelijke verbinding wordt de nieuwe norm. Met een veilige en stabiele internetverbinding werken je beter.

