VEILIG OP AFSTAND WERKEN VOOR HET MKB

Help uw medewerkers veilig thuiswerken met deze 10 TIPS

In een onvoorziene situatie zoals zich momenteel voordoet, is het mogelijk maken van thuiswerken essentieel voor de bedrijfscontinuïteit. Maar als er één ding is dat we weten over cybercriminelen, dan is het dat ze niet aarzelen om nieuwe kansen te benutten – vooral in tijden van crisis. Onvoldoende beveiligde thuiswerkmogelijkheden kunnen een organisatie kwetsbaar maken voor cyberaanvallen, met alle gevolgen van dien. Met deze tien tips beschermt u uw medewerkers en zorgt u voor een veilig thuiskantoor.

☐ Wees strikt in het wachtwoordbeleid

Als u tot nu toe niet heel strikt bent geweest op dit gebied, is dit het moment om het huidige beleid te herzien. Enkele suggesties: vereis voor ieder account een uniek en lang wachtwoord (of beter nog: een wachtzin), stel in dat een wachtwoord meerdere keren per jaar verplicht gewijzigd moet worden en blokkeer gebruikers na een x-aantal mislukte aanmeldpogingen. Hamer erop dat uw medewerkers wachtwoorden niet dienen te hergebruiken

☐ Schakel multifactorauthenticatie in (MFA)

Deze extra authenticatielaag (ook wel bekend als tweefactorauthenticatie of 2FA) bij het inloggen is de beste verdediging tegen cybercriminelen die bedrijfssystemen proberen te infiltreren met brute force-aanvallen, social engineering of gelekte inloggegevens die op het dark web zijn gekocht. Als u gebruikmaakt van zakelijke e-mail of samenwerkingstools in de cloud, of uw medewerkers op afstand toegang nodig hebben tot het zakelijke netwerk, implementeer dan een MFA-oplossing. Met ESET Secure Authentication voorkomt u ongeautoriseerde toegang tot bedrijfssystemen en -accounts. Deze MFA-oplossing kunt u snel en eenvoudig uitrollen – ook wanneer uw medewerkers thuiswerken.

☐ Gebruik een VPN voor toegang tot het bedrijfsnetwerk

Een VPN versleutelt zakelijk communicatieverkeer op het moment dat dit het openbare internet doorkruist, zodat het niet kan worden gelezen door derden. Als medewerkers op afstand toegang krijgen tot het interne bedrijfsnetwerk is de combinatie van een VPN met multifactorauthenticatie essentieel.

☐ Gebruik een virtual desktop interface indien mogelijk

Met gebruik van deze oplossing krijgen medewerkers toegang tot een virtuele machine, in de cloud of in uw lokale datacentrum. Zo'n machine kan geconfigureerd worden om het systeem op kantoor exact na te bootsen. Het voordeel van deze virtuele omgeving is dat gevoelige gegevens of bestanden alleen op de virtuele machine bestaan en dus nooit op het thuissysteem van de medewerker zijn opgeslagen.

☐ Herinner medewerkers aan risico's van netwerken en WiFi

Het thuisnetwerk van uw medewerkers, en de andere verbonden apparaten, liggen volledig buiten uw macht. Laat uw medewerkers het delen van bestanden uitzetten op het systeem dat ze voor werk gebruiken. Ook kunnen ze nagaan of hun thuisrouter of WiFi-toegangspunt WPA2-beveiliging aan heeft staan. Herinner ze daarnaast eraan om nooit met hun werksysteem verbinding te maken met een onbeveiligd of publiek WiFi-toegangspunt waarvoor geen wachtwoord nodig is.