

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 thuishkantoor.

- 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 datacenter. 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 thuisstelsel 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.

Investeer in een volledige oplossing voor endpointbeveiliging

Er zijn geen garanties dat de ingebouwde antivirussoftware van een privéapparaat voldoet aan de eisen van een organisatie, of dat je medewerkers überhaupt antivirussoftware hebben geïnstalleerd. Een volledige oplossing beschermt immers met meerdere verdedigingslagen tegen alle soorten cyberdreigingen, zoals een persoonlijke firewall, bescherming tegen schadelijke websites en malwarebescherming op verwijderbare USB-stations. De veiligste optie is om een zakelijke oplossing uit te rollen die uw IT-team op afstand kan beheren. Huidige zakelijke klanten van ESET kunnen nu tijdelijk hun huidige licentie gratis uitbreiden om medewerkers thuis dezelfde beveiliging te bieden als op kantoor. Voor meer informatie [kunt u contact opnemen met onze experts](#).

Maak gebruik van encryptie als medewerkers een zakelijke laptop mee naar huis hebben genomen

Bedrijfsapparaten worden niet alleen digitaal, maar ook fysiek aan een groter risico blootgesteld wanneer ze buiten de kantooromgeving worden gebruikt. Het is daarom raadzaam om alle zakelijke apparaten te beschermen tegen verlies en/of diefstal. Volledige schijfversleuteling zorgt ervoor dat de gegevens op de harde schijf in het gestolen of verloren apparaat vrijwel onmogelijk uit te lezen en dus te misbruiken zijn door onbevoegden. ESET Full Disk Encryption biedt sterke volledige schijfversleuteling op alle Windows-systemen en kan met één klik worden uitgerold, geactiveerd én beheerd op alle werkstations.

Maak uitloggen een gewoonte

Of ze nou een lunchpauze nemen, uitklokken of langer dan een paar minuten weg zijn van hun apparaat – het is belangrijk dat uw medewerkers uitloggen op het bedrijfsnetwerk. Deze vorm van digitale hygiëne is al helemaal een must als de computer gedeeld wordt of huisgenoten van uw medewerkers er bij kunnen.

Blijf scherp op patches en updates

Laat thuiswerkers op privéapparaten automatische updates van al hun systemen aanzetten, zodat u zeker weet dat alle veiligheidsmaatregelen geïnstalleerd worden. Wees extra voorzichtig met thuisapparaten waarop Windows 7 draait: dit besturingssysteem is verouderd en wordt niet meer geüpdatet. Het kan een keuze zijn om de toegang tot bedrijfssystemen voor deze gebruikers te blokkeren totdat het apparaat is geüpgraded naar een ondersteunde versie.

Bied medewerkers cybersecuritytrainingen

Ongeacht hoeveel technologie u ingeschakeld heeft, een belangrijk deel van beveiliging zit tussen de oren van uw medewerkers. Verdachte berichten van werk met het verzoek om inloggegevens of werk-gerelateerde websitebezoeken te bevestigen; verzoekjes van de baas om het overmaken van fondsen te faciliteren; deze en andere scams zullen vaker plaatsvinden nu cybercriminelen een slaatje proberen te slaan uit de vele thuiswerkers. Geïnformeerde, oplettende medewerkers zullen hier minder snel intrappen. Vooral bij werken op afstand zal een trainingsprogramma hen aansporen hierin alert blijven.

Thuiswerken gemakkelijker dan ooit

Cloud-gebaseerde productiviteitstools, online samenwerkingen via chat en videobellen en andere technologieën op afstand maken het mogelijk dat thuiswerkers hetzelfde productiviteitsniveau als op kantoor behouden – en soms zelfs productiever kun zijn. Wapen uw medewerkers niet alleen met de beste werkmogelijkheden, maar ook met de beste security.

Wilt u meer informatie over ESETs securityoplossingen? [Neem contact met ons op.](#)