VEILIG OP AFSTAND WERKEN VOOR HET MKB

Security-checklist voor werken op afstand

Het mogelijk maken van thuiswerken is vandaag de dag 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. Onvoldoende beveiligde thuiswerkfaciliteiten 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. Benadruk bij medewerkers dat wachtwoorden niet hergebruikt of uitgewisseld mogen worden.

☐ 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. Veel van deze oplossingen kunnen snel en eenvoudig worden uitgerold – ook als 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 indien mogelijk een virtual desktop interface

Bij 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 de risico's van netwerken en WiFi

Het thuisnetwerk en de andere verbonden apparaten van uw medewerkers liggen volledig buiten uw beheer. Laat medewerkers het delen van bestanden uitzetten op het apparaat dat ze ook voor werk gebruiken. Ook kunnen ze nagaan of hun thuisrouter of WiFi-toegangspunt WPA2-beveiliging aan heeft staan. Herinner ze er daarnaast aan om nooit met hun zakelijke apparaat 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 uw medewerkers überhaupt antivirussoftware hebben geïnstalleerd. Een volledige oplossing beschermt met meerdere verdedigingslagen – zoals een persoonlijke firewall, bescherming tegen schadelijke websites en malwarebescherming op verwijderbare USB-stations – tegen alle soorten cyberdreigingen. De veiligste optie is om een zakelijke oplossing uit te rollen die uw IT-team op afstand kan beheren.

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.

Maak van uitloggen een gewoonte

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

Hoeveel technologie u ook ingeschakeld heeft, een belangrijk deel van de verdediging tegen cyberdreigingen begint bij uw medewerkers. Verdachte zakelijke berichten met het verzoek om inloggegevens of werkgerelateerde websitebezoeken te bevestigen, verzoekjes van de baas om geld over te maken; 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 en verdachte zaken eerder melden. Vooral bij werken op afstand zal een training hen aansporen hierin alert blijven.

Thuiswerken gemakkelijker dan ooit

Productiviteitstools in de cloud, 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 werkfaciliteiten, maar ook met de beste security.