VEILIG OP AFSTAND WERKEN VOOR HET MKB

Handleiding Veilig op afstand werken voor het mkb

Nu grotendeels thuiswerken de nieuwe norm aan het worden is, kan het zijn dat de vraag opspeelt of uw organisatie in die vorm wel productief en veilig kan blijven. Veel grote bedrijven zoals Google en Microsoft omarmen deze verschuiving zonder grote tegenslagen, maar voor kleinere bedrijven en organisaties kan de situatie uitdagender zijn. Hoe zorg je ervoor dat de infrastructuur en het beleid aanwezig zijn om de bedrijfscontinuïteit te waarborgen?

Basisbenodigdheden

Allereerst zijn er, om productief te blijven, enkele algemene vereisten die alle thuiswerkende medewerkers nodig hebben:

- Een computer
- Goede internetverbinding
- Chat- en conferentietoepassingen
- Aparte werkruimte (bij voorkeur)
- Een zakelijke telefoon (optioneel)
- Motivatie en discipline
- Een routine

Naast deze fundering moeten bedrijven en organisaties zichzelf en hun werknemers ook voorbereiden op de **verhoogde cyberveiligheidsrisico's** die verbonden zijn aan werken op afstand.

Wat zijn enkele van de security-uitdagingen die moeten worden aangepakt?

1. Fysieke beveiliging van bedrijfsapparatuur
2. IT-beveiliging van het bedrijf als werknemers thuis werkzaam zijn
3. Inzicht in de technologische omgeving van thuiswerkers
4. Toegang krijgen tot het bedrijfsnetwerk en -systemen
5. Samenwerkingstools en autorisatieprocessen
6. Cybersecuritytraining
7. Ondersteuning en crisismanagement

1 Fysieke beveiliging van bedrijfsapparatuur

Bedrijfsapparatuur wordt blootgesteld aan een groter risico als ze de veiligheid en beveiliging van een fysiek kantoor verlaten. Deze apparaten moeten daarom worden beschermd tegen verlies en diefstal. Dit zijn enkele belangrijke maatregelen en tips om ervoor te zorgen dat alle apparaten beveiligd blijven:

- **Log uit als er niet gewerkt wordt** — zowel thuis als op openbare locaties. Een nieuwsgierig kind dat per ongeluk een e-mail naar de baas of een klant stuurt wordt hierdoor gemakkelijk voorkomen, net als de kans dat iemand toegang krijgt tot het apparaat terwijl u zich even op een andere locatie bevindt.
- **Sterk wachtwoordbeleid** — stel automatisch uitloggen bij inactiviteit in en verbied plaknotities met wachtwoorden erop (ja, mensen doen dit helaas nog steeds).
- **Laat apparaten nooit onbeheerd of op openbare plaatsen achter.**

PRO TIP

Volledige schijfversleuteling is een eenvoudige maar krachtige oplossing die ervoor zorgt dat zelfs als een apparaat in verkeerde handen valt, de bedrijfsgegevens niet toegankelijk zijn.

2 IT-beveiliging van het bedrijf als werknemers thuis werkzaam zijn

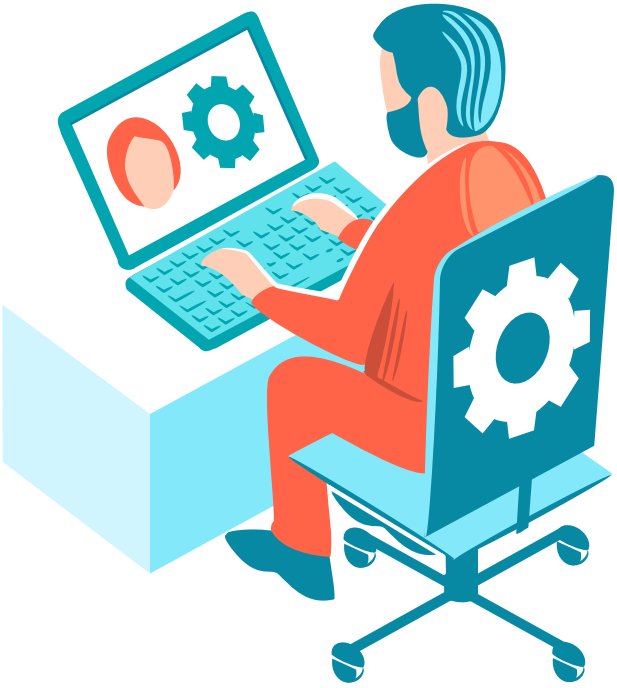
Als werknemers thuis aan het werk zijn, heeft u beperkt zicht op wat er gebeurt, vooral als u niet gewend bent apparaten op afstand te beheren en te monitoren. Dit is een goed moment om alle voordelen van extern beheer te leren kennen en het aantal IT-problemen waarmee u te maken krijgt aanzienlijk te verminderen.

Door extern beheer te gebruiken, bespaart u tijd.

- Configureer en onderhoud eenvoudig alle endpoints in één keer - zonder ze individueel af te hoeven gaan.
- Plan taken, definieer beleid en voer deze per groep of werknemer uit.
- Ontvang realtime meldingen over incidenten, zodat u onmiddellijk kunt reageren wanneer zich een incident voordoet.

PRO TIP

Als u over maximaal 250 apparaten beschikt, kunt u het bedrijfsnetwerk eenvoudig beheren via een cloudgebaseerde console. De activatie ervan duurt slechts enkele minuten. Meer informatie over een dergelijke oplossing vindt u hier.



3 Inzicht in de technologische omgeving van thuiswerkers

Vraag werknemers om hun eigen thuisnetwerk te controleren op kwetsbaarheden, voordat ze werkapparaten aansluiten. Er worden continu onderzoeken gepubliceerd over kwetsbare Internet of Things (IoT)-apparaten, en dit is een uitstekend moment voor werknemers om actie te ondernemen en deze te beveiligen met sterke wachtwoorden en hun firmware/software bij te werken naar de nieuwste versie.

Overweeg het gebruik van een app voor het monitoren van het thuisnetwerk te promoten of zelfs te verplichten voordat u werkapparaten met thuisnetwerken laat verbinden. Een dergelijke scan- of monitoringtool zal apparaten met bekende kwetsbaarheden, verouderde software of firmware of standaardwachtwoorden die gewijzigd moeten worden signaleren.

4 Toegang krijgen tot het bedrijfsnetwerk en -systemen

Stel vast of een werknemer toegang nodig heeft tot het interne netwerk van de organisatie of alleen toegang tot clouddiensten en e-mail. En denk erover na of hetzelfde toegangsniveau tot gevoelige gegevens moet worden verleend als een werknemer niet op kantoor is.

Als toegang tot het interne netwerk van de organisatie nodig is:

- Het wordt ten zeerste aanbevolen om alleen apparaten die eigendom zijn van de organisatie toegang te verlenen, zodat alle aangesloten apparaten onder het beheer vallen van het security- en IT-team.
- **Gebruik altijd een VPN** om externe medewerkers te verbinden met het interne netwerk van de organisatie. Dit voorkomt man-in-the-middle-aanvallen vanaf externe locaties. Houd er rekening mee dat bij thuiswerken het verkeer via openbare netwerken loopt.
- **Beheer het gebruik van externe apparaten** zoals USB-opslag en randapparatuur.
- Thuis of op kantoor; meer dan ooit zijn medewerkers doelwit van oplichting of phishing-e-mails. Met cloud sandboxing-oplossingen kunt u **verdachte e-mailbijlages en downloads buiten de apparaten** van werknemers houden.
- Beperk de mogelijkheid om gegevens op te slaan, te downloaden of te kopiëren. Een datalek kan plaatsvinden vanaf elk apparaat dat gevoelige bedrijfsgegevens bevat.
- Overweeg het gebruik van virtuele machines om toegang te verlenen. Dit kan ingewikkelder zijn om in te stellen, maar kan op de lange termijn de meest wenselijke oplossing zijn.

Als er medewerkers zijn die thuiswerken op een privé-apparaat en hiermee toegang krijgen tot e-mail- en clouddiensten, zorg er dan voor dat hetzelfde beveiligingsbeleid wordt doorgevoerd als op een zakelijk apparaat. Voorzie werknemers waar nodig van een licentie voor dezelfde security-oplossing die op kantoor gebruikt wordt. Neem contact op met uw leverancier als uw licentie hiervoor uitgebreid moet worden.

PRO TIP

Multifactorauthenticatie (MFA) zorgt ervoor dat alleen geautoriseerde gebruikers toegang krijgen, of het nu gaat om clouddiensten of volledig netwerktoegang. Gebruik waar mogelijk een mobiele applicatie of fysieke hardwaretokens om de eenmalige codes die geautoriseerde toegang verlenen te genereren.

5 Samenwerkingstools en autorisatieprocessen

Het lijkt misschien vreemd om deze twee items onder dezelfde kop te plaatsen, maar de ene kan problemen met de andere helpen voorkomen.

- Bied toegang tot chat-, video- en conferentiesystemen, zodat medewerkers met elkaar kunnen communiceren. Dit helpt werknemers de productiviteit hoog te houden én om sociaal te blijven met hun collega's.
- Gebruik samenwerkingstools om te beschermen tegen ongeautoriseerde instructies of transacties. Cybercriminelen kunnen thuiswerkend personeel misbruiken om Business Email Compromise (BEC)-aanvallen te lanceren. Dit zijn nep-dringende vragen, meestal om geld, die door kwaadwillenden per mail worden verzonden zonder de mogelijkheid om het verzoek persoonlijk te valideren.

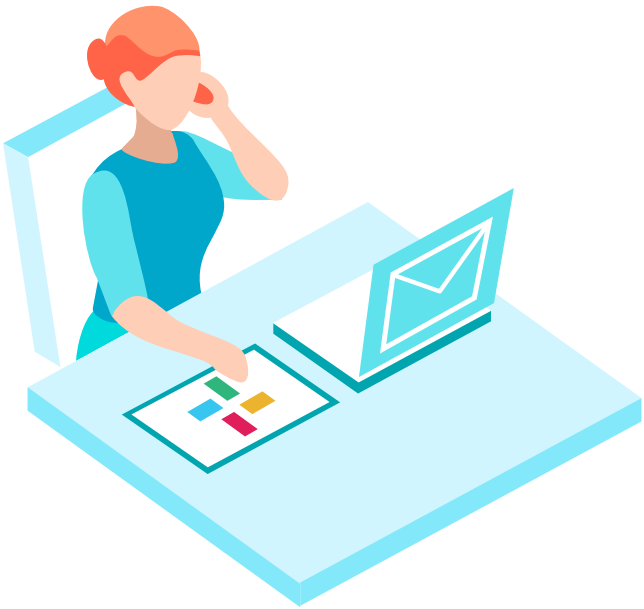
Zorg ervoor dat u videobellen / chatsystemen gebruikt als een formeel onderdeel van het goedkeuringssysteem, zodat er een "persoonlijke" check wordt gedaan, zelfs op afstand.

6 Cybersecuritytraining

Phishing-campagnes en social engineering worden steeds professioneler aangepakt en grootschaliger ingezet. In de meer ongedwongen sfeer van thuiswerken kunnen medewerkers zelfs sneller overwegen op links te klikken, omdat er geen collega's zijn die op hun scherm kunnen kijken. Het blijft daarom belangrijk om medewerkers te trainen in het herkennen van mogelijk risicovolle situaties en van hen de eerste verdedigingslinie tegen IT-bedreigingen te maken.

PRO TIP

Cybersecurity awareness training is vaak een jaarlijkse vereiste voor werknemers. Vooral als er veel op afstand wordt gewerkt, is het aan te raden om werknemers op willekeurige momenten te vragen een dergelijke training te volgen.



7 Ondersteuning en crisisbeheer

Thuiswerken mag nooit ten koste gaan van de cyberveiligheid of het netwerkbeheer van uw organisatie. De mogelijkheid om gebruikers op afstand te ondersteunen is daarbij essentieel. Thuiswerkende medewerkers moeten duidelijke communicatieprotocollen hebben voor IT-ondersteuning en crisisbeheer als ze ongebruikelijke of verdachte problemen tegenkomen die het gevolg kunnen zijn van een aanval.

Ga er niet vanuit dat alle werknemers effectief en met weinig hulp of begeleiding kunnen overschakelen naar thuiswerken. Thuis is niet het kantoor en ze hebben mogelijk hulp nodig om zich aan te passen.

Wilt u meer informatie over oplossingen voor veilig werken op afstand, neem dan contact op met uw securityleverancier of IT-partner om uw uitdagingen te bespreken.