VEILIG OP AFSTAND WERKEN VOOR HET MKB

Handleiding voor IT-beheerders; Veilig op afstand werken voor het MKB

Aangezien de COVID-19-pandemie veel werknemers dwingt om thuis te werken, kan het zijn dat de vraag opspeelt of uw organisatie productief en veilig kan blijven? Veel grote bedrijven zoals Google en Microsoft omarmen deze verschuiving zonder grote tegenslagen. Voor kleinere bedrijven en organisaties zal de situatie waarschijnlijk heel anders zijn.

Hoe zorg je ervoor dat de infrastructuur en het beleid aanwezig is om de bedrijfscontinuïteit te waarborgen?

Basis benodigdheden

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

- Computer
- Goede internetverbinding
- Chat- en conferentietoepassingen
- Speciale werkruimte (bij voorkeur)
- Optioneel een telefoon
- Zelfmotivatie en discipline
- Een strikte routine

Afgezien van de gebruikelijke opzet, moeten bedrijven en organisaties zichzelf en hun werknemers ook voorbereiden op de **verhoogde cyberbeveiligingsrisico's** die verbonden zijn aan werken op afstand.

Wat zijn enkele van de uitdagingen die moeten worden aangepakt?

1. Fysieke beveiliging van bedrijfsapparatuur
2. IT-beveiliging van het bedrijf wanneer werknemers thuis werkzaam zijn
3. Wat zit er in de thuis-technologie-omgeving?
4. Toegang krijgen tot het bedrijfsnetwerk en systemen
5. Collaboratieve tools en autorisatieprocessen
6. Cybersecurity-training
7. Ondersteuning en crisismanagement

1 Fysieke beveiliging van bedrijfsapparatuur

Werknemers zullen bedrijfsapparatuur blootstellen aan een groter risico wanneer ze de veiligheid en beveiliging van de werkplek verlaten. Apparaten moeten daarom worden beschermd tegen verlies en diefstal. Hier zijn enkele belangrijke maatregelen en tips om ervoor te zorgen dat alle apparaten beveiligd blijven.

- **Log uit wanneer niet in gebruik** - zowel thuis als op openbare plaatsen. 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 bevind.
- **Sterk wachtwoordbeleid** — stel time-outs voor inactiviteit in en verbied plaknotities met wachtwoorden erop (ja, mensen doen dit nog steeds).
- **Laat het apparaat nooit onbeheerd of op openbare plaatsen achter.**

PRO TIP

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

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

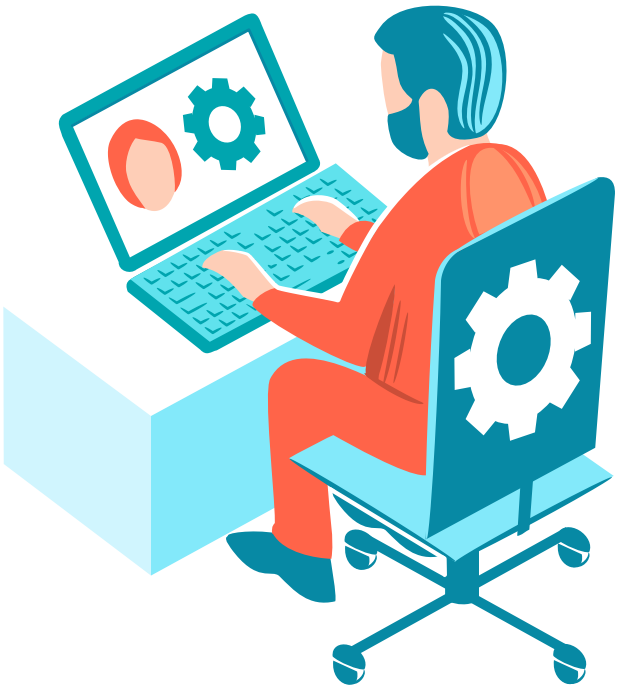
Nu werknemers thuis aan het werk zijn, heeft u beperkt zicht op wat er plaats vind, vooral als u niet gewend bent apparaten op afstand te beheren en te bewaken. Dit is een goed moment om alle voordelen van extern beheer te leren kennen en het aantal IT-problemen waarmee u te maken krijgt aanzienlijk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

Door extern beheer te gebruiken, bespaart u tijd.

- Configureer en onderhoud eenvoudig alle machinesystemen.
- Plan taken, definieer beleid en laat deze uitvoeren door verschillende groepen werknemers
- 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 netwerk van computers eenvoudig beheren via een cloud-gebaseerde console. De activering ervan duurt slechts enkele minuten. Meer informatie over zo'n oplossing vindt u hier.



3 Wat zit er in de thuis technologieomgeving?

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

Overweeg om het gebruik van een app voor het bewaken van een verbonden huis te promoten of zelfs te verplichten voordat u werkapparaten met thuisnetwerken kunt laten verbinden. De scan of monitoring zal apparaten markeren met bekende kwetsbaarheden, verouderde software of firmware of standaardwachtwoorden die moeten worden gewijzigd.

4 Toegang krijgen tot het bedrijfsnetwerk en systemen

Stel vast of de werknemer toegang nodig heeft tot het interne netwerk van de organisatie of alleen toegang tot Cloud gebaseerde services en e-mail. En houd er rekening mee of hetzelfde niveau van toegang tot gevoelige gegevens op locatie moet worden verleend wanneer de werknemer niet op locatie 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 organisatietoegang te verlenen, zodat de volledige controle over het aangesloten apparaat onder het beheer valt 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 afgelegen locaties. Houd er rekening mee dat, aangezien er nu vanuit huis gewerkt wordt, het verkeer nu over openbare netwerken stroomt.
- Beheer het gebruik van externe apparaten zoals USB-opslag en randapparatuur
- Omdat veel mensen thuis werken, worden ze het doelwit van oplichting of phishing-e-mails. Met voor cloud-sandboxing-oplossingen kunt u verdachte e-mails buiten de grenzen van machines 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 een superieure oplossing voor de langere termijn zijn.

Als sommige (of alle) werknemers BYOD (hun persoonlijke) apparaten gebruiken, zorg er dan voor dat als u hen toegang geeft tot e-mail- en Cloud services, u hetzelfde Endpoint security beleid voor antimalware, firewalls, enz. afdwingt als bij een apparaat dat door de organisatie wordt beheerd. 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 oplossing die op kantoor gebruikt wordt. Neem contact op met uw leverancier als uw licentie hiervoor uitgebreid moet worden. Zij hebben mogelijk initiatieven om ondersteuning te bieden tijdens deze bijzondere periode. Gebruikt u licenties van ESET en heeft u vanwege thuiswerkende medewerkers tijdelijk beveiliging nodig voor meer werkplekken, dan kunt u lopende zakelijke jaarlicenties tijdelijk kosteloos met maximaal 500 extra werkplekken uitbreiden.

PRO TIP

Multifactorauthenticatie (MFA) zorgt ervoor dat toegang, of het nu gaat om cloud-gebaseerde services of volledig netwerktoegang, alleen door geautoriseerde gebruikers is. Gebruik waar mogelijk een app-gebaseerd systeem of fysieke hardware token om eenmalige codes te genereren die geautoriseerde toegang verlenen.

5 Collaboratieve tools 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 biedt de benodigde productiviteitstools en helpt werknemers om sociaal te blijven met hun collega's.
- Gebruik de samenwerkingshulpmiddelen om te beschermen tegen ongeautoriseerde instructies of transacties. Cybercriminelen zullen waarschijnlijk de mogelijkheid van thuiswerkend personeel gebruiken om Business Email Compromise (BEC) -aanvallen te lanceren. Dit betreft een nep-dringende vraag welke wordt verzonden door een slechte actor, die om de dringende overdracht van geld vraagt, zonder de mogelijkheid om het verzoek persoonlijk te valideren.

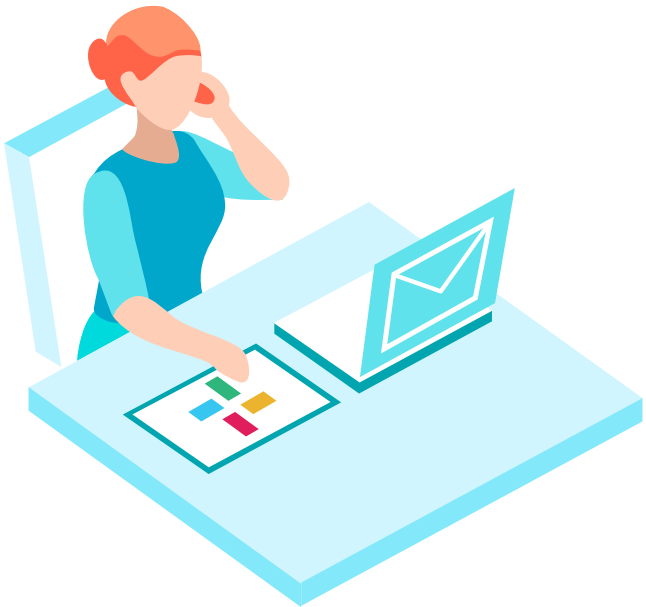
Zorg ervoor dat u videoconferenties / chatsystemen gebruikt als een formeel onderdeel van het goedkeuringssysteem, zodat de validatie "persoonlijk" wordt gedaan, zelfs op afstand.

6 Cybersecurity training

We zijn al getuige geweest van **talloze COVID-19-infecties** die in omloop waren, wat leidde naar gezichtsmaskers, vaccins en desinformatie. Wanneer werknemers de werkplek verlaten en in de meer ongedwongen sfeer van thuiswerken worden geplaatst, kunnen ze overwegen op links te klikken, omdat er geen collega's zijn die hen die grappige video kunnen zien bekijken of een webpagina kunnen bezoeken.

PRO TIP

Cybersecurity bewustzijnstraining is typisch een jaarlijkse vereiste voor werknemers. Vooral nu, wanneer er op afstand wordt gewerkt, is het aan te raden om een ad-hoc campagne uit te voeren en werknemers te vragen een dergelijke training te volgen.



7 Ondersteuning en crisisbeheer

In de haast om toegang op afstand te bieden, moet u zich bewust blijven van cybersecurity of de mogelijkheid om systemen en apparaten te beheren. De mogelijkheid om gebruikers op afstand te ondersteunen is essentieel voor een soepele werking, vooral als gebruikers vanwege gezondheidsredenen in quarantaine worden geplaatst. 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 mogelijke 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 aanzienlijke hulp nodig om zich aan te passen.

Hoe kan ESET helpen?

Als het gaat om beveiliging op de werkplek op afstand en de opkomende uitdagingen, kunt u vertrouwen op ESET. Hier zijn enkele van onze oplossingen die uw bedrijf helpen om in deze moeilijke tijden veilig en productief te blijven.

BEHEER OP AFSTAND

ESET Cloud Administrator

Door de Cloud beheerde beveiliging voor maximaal 250 stoelen, waardoor kosten en tijd worden bespaard en de bescherming van uw netwerk wordt vereenvoudigd.

- Installatie en implementatie binnen enkele minuten
- Geen extra hardware of software nodig
- Eén punt van netwerkbeveiligingsbeheer
- Overal veilig toegankelijk via een webbrowser

Ontdek nu

BEVEILIGDE APPARATEN

ESET Endpoint Protection

Meerlaagse technologie, machine learning en menselijke expertise gecombineerd met geautomatiseerd beveiligingsbeheer

- Eenvoudig te gebruiken beveiliging met cloudgebaseerd extern beheer
- Beschermt u tegen gerichte aanvallen, ransomware en bestandsloze aanvallen
- Add-on voor volledige schijfversleuteling

Ontdek nu

BEVEILIGDE TOEGANG

ESET Secure Authentication

ESET Secure Authentication
Een eenvoudige, effectieve manier voor bedrijven van elke omvang om multifactorauthenticatie te implementeren op veelgebruikte systemen.Hiermee kan uw organisatie:

- Datalekken voorkomen
- Voldoen aan compliance vereisten
- Centraal beheren vanuit uw browser
- Gebruik maken van telefoon of hardware tokens

Ontdek nu

Voor meer informatie over oplossingen voor werken op afstand, bezoek onze speciale webpagina.