ProteQtor
Next-Gen IT Security

VEILIGER THUISWERKEN

Maatregelen voor organisaties en thuiswerkers om het thuiswerken te beschermen tegen hackers.

Hoe thuiswerken veiliger maken?

Door het coronavirus ging menigeen zoveel mogelijk thuiswerken om de verspreiding van het virus tegen te gaan. Nadat de maatregelen versoepeld werden, konden we weer naar kantoor of andere werklocaties terugkeren. Maar thuiswerken blijft voor velen nog een voorwaarde of een alternatief voor kantoor. In het Okta onderzoek De nieuwe werkplek: het herinrichten van werk na 2020 bleek de helft van de Nederlanders voor de Coronacrisis nooit thuis te hebben gewerkt. Maar door het gedwongen thuiswerken heeft een groot deel van de kantoormedewerkers het alternatief voor op kantoor werken kunnen ervaren. 39% van de Nederlandse ondervraagden wil in het vervolg het liefst flexibel werken waarbij deels thuis gewerkt wordt.

Maar met thuiswerken wordt de veiligheid van het bedrijfsnetwerk omgeruild voor het veelal minder veiligere IT-omgeving van thuis. Toen de Coronacrisis uitbrak, bleek dat veel organisaties de online beveiliging van hun thuiswerkers niet op orde hadden. Slechts 1 op de 5 ondervraagde Nederlandse werknemers heeft vertrouwen dat hun werkgever volledig voorbereid is op het gebied van online beveiliging. Rond 80% van de thuiswerkers heeft het gevoel dat ze in meer of mindere mate onveilig moeten thuiswerken. Met de toegenomen cyberaanvallen is het van groot belang dat de online beveiliging voor thuiswerkers goed geregeld wordt.

In dit document sommen we een aantal maatregelen die zowel de organisatie als de thuiswerker kunnen nemen om die online beveiliging te verbeteren. Deze maatregelen zijn gebaseerd op een aantal aanbevelingen van het **Nationaal Cyber Security Centrum (NCSC)** samengevoegd met de aanbevelingen van andere (buitenlandse) instanties zoals de New Jersey Cybersecurity & Communications Integration Cell. Tot slot hebben we een aantal eigen aanbevelingen toegevoegd. Vervolgens sommen we een aantal tools op die deze maatregelen ondersteunen.

Maatregelen om uw medewerkers en daarmee uw organisatie tegen hackers te beschermen

- Stel een **BYOD (Bring Your Own Device) beleid** op. Waar moet een eigen mobiel, tablet, laptop en/of desktop aan voldoen om informatie van de organisatie te verwerken?
- Zorg voor **voldoende (netwerk)capaciteit**, zodat alle thuiswerkers ook goed kunnen werken.
- Zorg dat uw thuiswerkers gebruik maken van een **Virtual Private Netwerk (VPN)** of een andere veilige thuiswerkoplossing om verbinding te maken met het bedrijfsnetwerk.
- Zorg dat de medewerker thuis ook de **password manager** van werk kan gebruiken.
- Zet waar mogelijk **Multi-Factor Authenticatie (MFA)** aan.
- Indien medewerkers van veel verschillende applicaties gebruik moeten maken, dan is een **identity manager met SSO Single Sign On (SSO)** een optie. Deze hebben veelal ook monitoringsmogelijkheden om te zien wat de activiteiten van de thuiswerkers zijn.
- Pas een **NAC Network Access Control** oplossing toe als remote devices toegang tot het interne bedrijfsnetwerk moeten krijgen.
- Installeer de meest **recente updates** voor hard- en software.
- Check de **privileges** die gebruikers hebben bij SaaS-producten en andere applicaties. Waar ze op kantoor wél informatie mochten bekijken, aanpassen, downloaden en verwijderen, is dit wellicht onwenselijk vanuit thuis apparaten. Om datalekken te voorkomen is het essentieel dat thuiswerkers geen bedrijfsgevoelige gegevens en persoonsgegevens kunnen downloaden. Veelal bieden cloud service providers de mogelijkheid om het downloaden van data tegen te gaan. Wordt die mogelijkheid niet geboden, dan is een **Cloud Access Security Broker (CASB)** een oplossing omdat die de benodigde controlemogelijkheden biedt.
- Zorg dat de thuiswerkende medewerkers uitgerust zijn met **endpoint protection voor hun mobiele apparaten, hun laptops en/of desktops** om cyberaanvallen op hun apparaten af te weren.
- Zorg voor een zo **veilig mogelijk e-mailsysteem**, zodat medewerkers zo min mogelijk geconfronteerd worden met kwaadaardige e-mails en dat de kans op het onderscheppen van e-mails geminimaliseerd wordt.
- Bied thuiswerkers een crash course **cybersecurity awareness** door ze te wijzen op gevaren van phishing e-mails en andere kwaadaardige social engineering. Er is een hausse aan Coronavirus-gerelateerde scams die onder het mom van informatie over de virus malware, zoals de wachtwoordstelende AZORult, bij onoplettenden plaatsen.

Hoe kan ik het werken bij mij thuis veiliger maken?

Maatregelen voor de thuiswerker

- Maak gebruik van een **vertrouwd en beveiligd (wifi-)netwerk**. Zorg dat u wifi beveiligd is met beveiligingsmodus (WPA-PSK2).
- Log alleen in met een **password manager met waar mogelijk 2-factor authenticatie (2FA) of Multi-factor Authenticatie (MFA).**
- Als u nog logins heeft zonder multi-factor authenticatie, stel deze dan gelijk in indien die mogelijkheid geboden wordt.
- Controleer dat u alleen op het bedrijfsnetwerk inlogt als u zeker weet dat **het VPN en de endpoint protection ingeschakeld** staan.
- Houd rekening met tragere applicaties door een langere reactiesnelheid.
- Houd er rekening mee dat u **phishing en nep e-mails over het Coronavirus** kunt ontvangen. Ontvangt u deze, meld deze dan bij uw IT-beheerder. Ga niet in op de phishingmail.
- **Klik niet op links in e-mailberichten**, open geen onbekende bijlagen en vul geen gegevens in bij e-mailberichten die u niet verwacht of van een onbekende afzender zijn.
- Houd de **organisatierichtlijnen aan betreffende informatiebeveiliging**. Ga bewust om met informatie thuis en wat u bespreekt in berichtenapps of tijdens een videoconference. Daar hoort ook bij het maken van beeldopnames van de thuiswerkplek die dan op sociale media geplaatst worden.
- Volg de **richtlijnen van de organisatie omtrent gebruik van hard- en software**. Denk aan gebruik van privé- en randapparatuur en het installeren van applicaties. Een voorbeeld is de malafide app ‘COVID19 Tracker’ deze installeert de CovidLock ransomware op apparaten met het Android besturingssysteem.

Welke tools heb ik nodig?

Hoe dicht u de gaten in uw security?

Als u merkt dat u niet alle maatregelen kunt nemen, terwijl u het wel nodig vindt dat ze genomen worden, dan kunnen we u bij een aantal helpen. We hebben een **Thuiswerk Security Pakket** opgesteld, dat bestaat uit een aantal cybersecurity tools (klik op de rode link voor meer info over die tool):

- **Password managers** om complexe wachtwoorden te maken en te beheren.
- **Multi-Factor Authenticatie apps** om meerdere lagen beveiligingen aan wachtwoorden te geven.
- **Endpoint Protection app voor mobiele apparaten** om smartphones en tablets tegen cyberaanvallen te beschermen.
- **Endpoint Protection software voor laptops en desktops** om pc's maar ook (virtuele) servers tegen cyberaanvallen te beschermen.
- **Webfiltering** om vooraf gevaarlijke websites en e-mails uit te filteren..
- **E-mail Security** om beveiligd e-mails te ontvangen en te versturen.
- **Cybersecurity Awareness Trainingen** om medewerkers cyberaanvallen te leren herkennen en er mee om te gaan.

Ons Thuiswerk Security Pakket betaalt u per maand of per jaar (u krijgt 5% korting).
U kunt ook uw Thuiswerk Security Pakket zelf samenstellen met een Pakket Op Maat .

Meer info over onse Thuiswerk Security Pakket? Klik hier.

Samen de weerbaarheid van uw thuiswerkers verhogen

Uit het Okta-onderzoek blijkt dat een meerderheid van op kantoor werkend Nederland een flexibelere regeling wil waarbij ze deels vanuit huis kunnen werken. Deze flexibiliteit levert wel uitdagingen op het gebied van online beveiliging. Ons Thuiswerk Security Pakket helpt bij die uitdaging.

Kunt u wel wat hulp gebruiken?

Bel 088-0660770 of plan een afspraak in

Hulp nodig bij het samenstellen van uw Thuiswerk Security Pakket? Wilt u advies hoe u uw organisatie het beste kunt beschermen? Bel ons vrijblijvend op 088-0660770. Of plan zelf uw afspraak voor een telefoon/videogesprek in. Dan kijken we samen wat voor u de beste oplossingen zijn om uw organisatie veel weerbaarder te maken.

ProteQtor
Next-Gen IT Security

Telefoon : +31 (0)88 066 0770
E-mail : contact@proteqtor.nl
Website : proteqtor.nl