ProteQtor
Next-Gen IT Security

VEILIGER THUISWERKEN TIJDENS DE CORONACRISIS

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

Hoe kunt u veiliger thuiswerken?

Door het coronavirus wordt iedereen door de regering opgeroepen zoveel mogelijk thuis te werken. Dit om de kans zoveel mogelijk te verkleinen dat anderen besmet worden. Maar met thuiswerken wordt de veiligheid van het bedrijfsnetwerk omgeruild voor het veelal minder veiligere IT-omgeving van thuis.

De gevaarlijke mix van enerzijds thuiswerkers die vanuit een veel onveiligere omgeving toegang krijgen tot uw bedrijfsgegevens en anderzijds een toename van hackeractiviteiten gericht op het verkrijgen van uw bedrijfsgegevens of uw geld via het gijzelen van uw bedrijfsgegevens, zorgt ervoor dat er beschermende maatregelen genomen moeten worden door de organisatie én de thuiswerker.

Het **Nationaal Cyber Security Centrum (NCSC)** heeft een aantal aanbevelingen gedaan die we hebben 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. In de volgende pagina's ziet u de maatregelen op een rijtje, gesplitst naar organisatie en thuiswerker.

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.
- Maak een **beoordeling** van welke medewerkers op kantoor moeten zijn om de thuiswerkers te kunnen ondersteunen met hun IT-voorzieningen.
- Bedenk welke aanpassingen mogelijk nodig zijn voor uw **incident respons plannen** bij een beperkte aanwezigheid van medewerkers.
- 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 te plaatsen.

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.

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.
- **Secure Virtual Private Network (VPN) verbindingen** om thuiswerkers veilig met het bedrijfsnetwerk en cloud-omgevingen te laten verbinden.
- **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.

U kunt uit diverse Thuiswerk Security Pakketten kiezen: **Basis**, **Aanvullend** en **Uitgebreid**. U kunt ook zelf een pakket samenstellen.

Meer info over onze Thuiswerk Security Pakketten? Klik hier.

Samen de weerbaarheid van uw thuiswerkers verhogen

Niemand weet hoe lang de Coronacrisis gaat duren en dus hoe lang uw medewerkers vanuit huis moeten werken. Dan is het maar beter om een veilige thuiswerksituatie te creëren, zodat de druk op de organisatie niet verder opgevoerd wordt door een hack. Onze Thuiswerk Security Pakketten zijn een goede basis. Kies welke het beste bij uw organisatie past.

Kunt u wel wat hulp gebruiken?

Bel 088-0660770 of plan een afspraak in

Hulp nodig bij het kiezen welke Thuiswerk Security Pakket het beste voor uw organisatie is? Bel ons vrijblijvend op 088-0660770. Of plan zelf uw afspraak voor een telefoon/videogesprek in. Samen kijken we wat voor u de beste oplossingen zijn en samen zorgen we dat uw organisatie veel weerbaarder wordt.

ProteQtor
Next-Gen IT Security

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