BDO RISK ADVISORY

VEILIG TELEWERKEN

De voorbije vijf weken voerden bedrijven thuiswerk verplicht in waar het kon, wat leidde tot een vervijfvoudiging van het aantal Belgen dat zijn job vanuit zijn kot deed. Het versneld invoeren van telewerk was voor sommige organisaties een heuse uitdaging, maar het thuiswerk in tijden van corona smaakt duidelijk naar meer. Negen op de tien Belgische werknemers en leidinggevenden zien zo'n 1 à 3 dagen per week wel zitten na de versoepeling van de coronamaatregelen. Zes op de tien zelfs 2 dagen of meer.

Of hoe een niet te voorspellen pandemie ook een aantal positieve evoluties met zich mee kan brengen. Telewerk is al jarenlang een nieuwe manier van werken die vele bedrijven willen implementeren, maar vaak uitstellen of niet volledig uitrollen. De huidige crisis dwingt hen echter om deze sprong in het diepe te maken. Iets waar ze zeker kritisch naar moeten kijken zijn de veiligheidsimplicaties van deze transformatie.

NIEUWE VEILIGHEIDSRISICO'S

Telewerken doe je niet zonder risico. Zo zijn medewerkers kwetsbaarder voor social engineeringaanvallen bij thuiswerk (zoals meer afleiding, minder focus, minder fysiek en verbaal contact met collega's, etc.). Verder impliceert telewerk een connectie tot het netwerk van de werkgever, een kanaal dat hackers maar al te graag uitbuiten. Tenslotte stoten medewerkers vaak op praktische problemen (zoals het uitwisselen van informatie met collega's) waarvoor ze bij gebrek aan goede tools of duidelijke richtlijnen soms onveilige oplossingen gebruiken.

NIEUWE MAATREGELEN EN RICHTLIJNEN

Er zijn gelukkig een aantal maatregelen om als organisatie deze nieuwe risico's te beperken:

- **Een teleworking policy**, die duidelijke richtlijnen omvat op vlak van organisatie, technologie en veiligheid.
- **Het opkrikken van de waakzaamheid van de medewerkers** via campagnes, eventueel gecombineerd met gesimuleerde social engineering aanvallen om het risicobewustzijn verder te vergroten.
- **Het onderwerpen van de gebruikte telewerktechnologie aan doorgedreven veiligheidstesten**. Mogelijke kwetsbaarheden worden zo tijdig blootgelegd en opgelost.

Daarnaast moeten de werknemers duidelijke instructies krijgen over:

- Het **gebruik van software** in een telewerkcontext. Je laat best enkel software toe die door het interne IT-departement wordt aangereikt (zoals Filesharing en online opslag, video conferencing, collaboratieve werkplekken, etc.). Zogenaamde gratis platformen kunnen een aantrekkelijke optie lijken, maar achterliggend een risico betekenen voor de beveiliging of privacy van je data. Denk maar aan de veiligheidsproblemen die het populaire Zoom met zich meebracht.
- **Toestellen waarmee ze connecteren**. Dat is enkel mogelijk vanop een toestel van de werkgever of vanop een eigen toestel dat aan een aantal voorwaarden voldoet (zoals anti-malware software, versie van het besturingssysteem en de veiligheidsupdates, wachtwoordbeveiliging, etc.).
- **Het thuisnetwerk**: tijdens de lockdown is een internetcafé alvast geen optie, en dus meteen ook een risico minder om te beheren. Over de beveiliging van het thuisnetwerk daarentegen kunnen veel medewerkers nog wat praktische tips en tricks gebruiken. Hebben ze de standaardwachtwoorden van de netwerkapparatuur veranderd? Hebben ze de laatste beveiligingsupdates toegepast? Is hun draadloze netwerk voldoende sterk beveiligd? ...

Telewerk is een belangrijk onderdeel van de 'New Normal'. Ook jouw organisatie zal zich danig moeten aanpassen aan de nieuwe manier van werken en zakendoen. Met deze nieuwe maatregelen en richtlijnen zorg je ervoor dat dit op een veilige wijze gebeurt.

Interesse?

Neem contact op met:

FRANCIS OOSTVOGELS
Manager Risk Advisory Services

E-mail: francis.oostvogels@bdo.be
Tel.: +32 474 92 08 00

NICK HUYSMANS
Manager Risk Advisory Services

E-mail: nick.huysmans@bdo.be
Tel.: +32 486 31 90 45