VEILIG THUIS EN MOBIEL WERKEN

In 2020 is de digitale transformatie waar het gaat om online vergaderen en contacten als gevolg van de coronacrisis in een stroomversnelling terecht gekomen. Na wat aanloopproblemen ervaren veel mensen de voordelen van het mobiele werken. En hoewel er ook nog wel op kantoor wordt gewerkt, is de verwachting dat thuiswerken/mobiel werken een blijvertje is. In dit artikel aandacht voor het onderwerp.

WACHTWOORDSCAN

Er worden steeds meer online applicaties gebruikt. De hiervoor gebruikte wachtwoorden zijn vaak onvoldoende veilig. Bovendien is vaak niet duidelijk welke online applicaties worden gebruikt binnen het kantoor. Met de SRA Wachtwoordscan krijgt u hier inzicht in. Kijk voor meer informatie op sra.nl/wachtwoordscan.

Accountantskantoren opereren meer en meer in een gedigitaliseerde omgeving. Data en informatie gaan meer dan ooit over organisatiegrenzen heen. Informatiebeveiliging, cybersecurity en privacy van het kantoor gaan dan ook verder dan alleen het fysieke pand. Vanuit wet- en regelgeving, maar ook door klanten, wordt verwacht dat organisaties passende maatregelen treffen om de continuïteit en de betrouwbaarheid van data en IT-systemen te waarborgen, risico's te mitigeren en gevolgen van eventuele beveiligingsincidenten zoals datalekken te beperken. Desondanks is de aandacht voor informatieveiligheid nog steeds minimaal.

SECURITYTRENDS

Tegelijkertijd zijn er een aantal securitytrends waar te nemen. Een aantal hiervan is ook te relateren aan het thuiswerken:

- **Ransomware**
  Thuisnetwerken zijn minder goed beveiligd dan bedrijfsnetwerken. Via het thuisnetwerk proberen cybercriminelen toegang te krijgen tot het bedrijfsnetwerk.
- **Phishing**
  Doordat we thuiswerken krijgen we meer e-mail. Cybercriminelen gebruiken bovendien onze hang naar informatie over actuele onderwerpen, zoals het coronavirus, om zo spyware en malware te installeren.
- **Veiligheidscultuur binnen organisaties wordt belangrijker**
  Informatiebeveiliging, cybersecurity en AVG gaan over de digitale veiligheid van de organisatie en zijn daarmee een directieverantwoordelijkheid. Thuiswerken valt hier ook onder.
- **Datalekken en privacyincidenten nemen toe.**
  Als gevolg van het vele thuiswerken gaat vrijwel alle informatie-uitwisseling digitaal, veelal per e-mail.

Het is niet alleen van belang hiervan bewust te zijn, maar ook maatregelen te treffen.

VEILIG TERUGKEREN NAAR KANTOOR

Of het kantoor nu meer een ontmoetingsplaats wordt of weer een traditioneel kantoor wordt, één ding is zeker: we keren op enig moment weer terug naar kantoor en loggen dan weer direct in op het bedrijfsnetwerk. Voordat dit wordt gedaan, is het belangrijk een aantal dingen te realiseren en zeker ook te controleren:

- Software is niet (meer) up-to-date omdat thuis updaten niet mogelijk was of niet is gedaan. Controleer of alle (Windows)updates zijn gedaan. Installeer deze, waar dit nog niet is gedaan.
- Laptops bevatten ongeautoriseerde, mogelijk illegale software. Verwijder deze software.
- Laptops zijn geïnfecteerd met malware. Scan de computers, nadat ook de virusscanner is geüpdatet.
- Check medewerkers met afwijkende gebruiksrechten. Soms zijn deze rechten tijdelijk ingesteld, maar vergeten in te trekken.
- Controleer uitgeschakelde maatregelen zoals updates, firewall, virusscanners, encryptie, etc.

EEN VEILIGE MOBIELE WERKPLEK

Thuiswerken en/of mobiel werken brengt risico's met zich mee. Thuisnetwerken zijn over het algemeen minder goed beveiligd dan bedrijfsnetwerken. Door de vervaging van grens tussen zakelijk en privé is de kans groot dat de bedrijfslaptop wordt gebruikt voor (onveilige) privéactiviteiten.

Een belangrijk advies van het Nationaal Cyber Security Centrum in dit kader is na te gaan welke van uw kritieke bedrijfsprocessen geheel of gedeeltelijk steunen op thuiswerken. Welke mogelijk risico's en bedreigingen zijn direct gerelateerd aan het thuiswerken en welke mitigerende maatregelen kunnen worden genomen? Denk hierbij ook aan duidelijke communicatie en richtlijnen voor uw medewerkers van het hoe en waarom van bepaalde maatregelen.

> **“VIA HET THUISNETWERK PROBEREN CYBER-CRIMINELEN TOEGANG TE KRIJGEN TOT HET BEDRIJFSNETWERK.”**

Enkele maatregelen die u samen met uw medewerkers in dit kader kunt nemen:

- Verhoog het bewustzijn bij medewerkers. Zorg ervoor dat men weet welke informatie mag worden gedeeld, met wie en op welke wijze.
- Update regelmatig de betrokken apparatuur. Sluit de computer aan het einde van de dag af. Dit zorgt ervoor dat kritieke updates worden doorgevoerd.
- Denk aan (extra) back-ups bij lokaal werken.
- Geef richtlijnen voor het gebruik van tools voor videoconferencing, zoals MS Teams en Zoom.
- Schrijf op wat u (anders) doet. Dit betreft niet alleen incidenten, maar ook zaken die anders gaan of moeten gaan dan op kantoor.
- Zorg voor veilige verbindingen. Maak gebruik van een vertrouwd en beveiligd (wifi)netwerk. Gebruik multifactor authenticatie en/of VPN-verbindingen.
- Hanteer ‘vaste’ werktijden en een clean-deskpolicy.
- Laat computers niet onbeheerd achter en lock de computer (⊞ + L). Voorkom dat door onbevoegden toegang wordt verkregen en (onbewust) schade wordt aangebracht in bedrijfsapplicaties.

Wat tot slot niet moet worden vergeten, is de medewerker. Thuiswerken kan zeker in die situaties waarin het noodgedwongen is, ook leiden tot eenzaamheid of een sociaal isolement. Zorg ervoor dat mensen betrokken blijven. Af en toe een online meeting om even bij te praten of een online pubquiz houdt mensen betrokken.

MEER WETEN EN HOE NU VERDER?

Ga naar de dossierpagina AVG en Privacy op sra.nl, voor alle vragen en antwoorden en beschikbare documenten. Of neem contact op met Tony van Oorschot, automatisering@sra.nl of 030 656 60 60.

RISICOKLASSENINDELING DIGITALE VEILIGHEID

Om mkb-bedrijven te helpen heeft het Digital Trust Center (onderdeel van ministerie van Economische Zaken) een gratis risicoclassificatiemodel ontwikkeld. Aan de hand van elf vragen wordt niet alleen een inschatting gegeven van het risico op een cyberincident, ook wordt aangegeven welke maatregelen kunnen worden genomen om de digitale veiligheid te vergroten. Kijk voor meer informatie op www.digitaltrustcenter.nl/risicoklasse.

VOORZORGSMAATREGELEN VOOR HET AANLEVEREN VAN ADMINISTRATIES/PAPIEREN DOSSIERS

Vraag uw klant de administratie/dossiers af te laten leveren door iemand die geen verschijnselen heeft van verkoudheid of griep. Of vraag om een digitale aanlevering.

Spreek met de klant een datum/tijdstip af waarop deze de administratie komt aanleveren.

Vraag uw klant om alleen te komen.

Maak een plaats, bij voorkeur in een aparte ruimte, beschikbaar waar de klant de administratie kan neerzetten. Denk hierbij aan een tafel met daarop een A4 met naam van de klant.

Vraag de klant te melden als deze is gearriveerd zodat medewerkers weten dat iemand komt. Als de deur van het kantoor gesloten is, kan deze worden geopend.

Zorg voor ten minste 1,5 meter afstand.

Raak alleen de stukken aan die u nodig heeft. Reinig mappen en/of ordners (met een desinfecterende doek) voordat deze worden opgeborgen in het klantarchief.

Zorg ervoor dat de klant de aanwijzingen opvolgt.

Hanteer bij het ophalen van de administratie/dossiers dezelfde procedure zoals hierboven beschreven.