centrum informatiebeveiliging en privacybescherming

Handreiking Veilig Thuiswerken

Tips voor organisaties en advies aan medewerkers (incl. checklist voor thuis)

April 2021 [versie 1.0]

Handreiking Veilig Thuiswerken

Titel	Handreiking Veilig Thuiswerken
Datum	April 2021
Status	Versie 1.0
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	Yosta Dammen, op basis van een webinar over Veilig Thuiswerken vanuit de CIP CISO Cirkel, met Michiel Dirriwachter, Rik Driessen en Jeroen Simons

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt.

Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Veilig Thuiswerken

Hoe doe je dat? Waar moet je op letten? Welke praktische tips en trucs zijn er?

De aanleiding: zakelijk gebruik video-vergaderen

Sinds maart 2020 werken vrijwel alle medewerkers van overheidsorganisaties als gevolg van de COVID-19 crisis vanuit huis. Door het thuiswerken zijn de mogelijkheden om video-vergaderingen te kunnen ondersteunen en webinars te kunnen geven in heel korte tijd ineens onmisbaar geworden. Helaas werken de, binnen de overheid gebruikte, tools die hiervoor zijn uitgerold alleen buiten de Citrix- (of een andere beveiligde) omgeving. Om de bedrijfsvoering te ondersteunen zijn de reeds geplande implementaties van video-vergader tools zoals MS Teams, Webex, Zoom, Skype, enz. versneld, of nam het gebruik ervan sterk toe. Door de overhaaste uitrol van nieuwe tooling c.q. samenwerkingsverbanden is er soms minder aandacht aan security- en privacyaspecten besteed.

Nu deze tools de norm zijn geworden, werken overheidsmedewerkers steeds vaker buiten de veilige Citrix-omgeving zonder tweefactor-authenticatie (2FA), op eigen computers en/of in de cloud, deels buiten het centrale beheer van de werkgever. Dit brengt reële beveiligingsrisico's met zich mee. Om die risico's te mitigeren hebben we onderzocht welke mitigerende maatregelen extra aandacht zouden moeten krijgen. Nu we ruim een jaar gebruik maken van deze tooling, is het zeker zinvol om deze tools – ook vanuit proces en organisatie - nogmaals tegen het licht te houden qua beveiliging. Doordat vanuit de centrale organisatie minder zicht is op de gedragingen van medewerkers blijft het zaak hen te wijzen op hun eigen verantwoordelijkheid op het gebied van informatiebeveiliging. Door hen aan te geven wat ze zeker niet moeten doen, kan veilig gedrag positief worden beïnvloed.

Tips voor organisaties en verantwoordelijken

Vanuit iedere organisatie is vaak een CISO, CIO, informatiemanager of IB-specialist verantwoordelijk voor het beleid op het gebied van informatiebeveiliging, het stellen van eisen aan de informatiebeveiliging en het toetsen of de gebruikte tools blijvend voldoen aan de eisen die gesteld worden vanuit dat beleid. Bij iedere verantwoordelijke zal, ook voor video-conferencing tools, sprake dienen te zijn van risico-bewustzijn.

Doordat het gebruik van video-conferencing tools een vlucht heeft genomen waarbij het belang van deze tools voor de organisatie is toegenomen, is het zaak deze tools te her-classificeren en wellicht zelfs wel te her-contracteren, rekening houdend met de BIV (Beschikbaarheid, Integriteit en Vertrouwelijk). Het gebruik van een BIO BBN toets (classificatie van informatie) geeft inzicht in het veranderde belang van het tool. Waarbij het met name gaat over de mate van vertrouwelijkheid van de verwerkte informatie. Met de leverancier dienen aanvullende afspraken te worden gemaakt (waar mogelijk) om de informatiebeveiliging op niveau te brengen en te houden. Of inkoop dient te geschieden via organisaties die zulke afspraken al hebben gemaakt.
Verder horen gebruikers heldere instructies te krijgen over wat wel en wat niet te delen tijdens video-vergaderen. Ook dienen gebruikers te worden gestimuleerd zich risicobewust te gedragen.

Proces-tips

Vanwege het veranderde gebruik zal er volop aandacht moeten zijn voor de Risicomanagement processen ten aanzien van informatiebeveiliging op de thuiswerkplek.

Bij de heroriëntatie vanuit de organisatie zal het management rekening moeten houden met veiligheidsvraagstukken en mogelijke dreigingen. Met andere woorden:

- Hoe om te gaan met extra functionaliteiten in applicaties? Zetten we centraal opties aan of uit? Met de voorkeur voor 'uit', om de medewerkers niet onbedoeld teveel ruimte te geven. Of wijzen we de medewerker op het juiste gebruik van de opties;
- Hoe wordt omgegaan met het uitdijende app(-licatie)landschap? Welke tools staan we toe? Op basis van IB&P regels. Geef duidelijke richtlijnen over het gebruik van publieke gratis tools;
- Hoe kan de "decentrale informatie" (Informatie management, Identity en Acces Management, Data Life Cycle Management (incl. verwijderen/archiveren) en Veiligheid & Privacy worden beheerst?
- Wat wordt toegestaan en wat verboden? Moeten er aanvullende afspraken (geheimhouding) met de medewerkers worden gemaakt?
- Zorg dat kwaadwillenden geen toegang kunnen krijgen via de thuiswerkplek van de medewerker. Zorg voor voldoende beveiliging en bewaak/stimuleer dat de juiste tools en aangeboden beveiligingsupdates (van bijvoorbeeld Windows of Adobe) meteen worden geïnstalleerd en blijvend gebruikt;
- Vergroot de awareness rondom de tooling. Maak medewerkers opnieuw alert op spam, phishing en ransomware. Medewerkers moeten veiligheidsincidenten of datalekken gewoon blijven melden, mogelijk is hier een procesaanpassing voor nodig. Creëer een veilig klimaat om incidenten te melden. Biedt ook ondersteuning voor medewerkers voor hun zakelijke én thuiswerkplek en privé-apparatuur, bijvoorbeeld met een helpdesk, intranetpagina's, tips & tricks, FAQ's, e.d. En evalueer periodiek de informatieveiligheid van de thuiswerkplek.

Advies aan medewerkers

Doordat iedereen vanaf maart 2020 zoveel mogelijk thuis werkt, zijn de organisatie en medewerkers op zoek gegaan naar mogelijkheden om het werk zo makkelijk mogelijk te verrichten. Dat kan zijn via de door de werkgever verstrekte middelen (laptop, telefoon, printer, enz.) of via privé middelen die toch al beschikbaar waren.
Omdat gebruik van eigen apparatuur en programma's (download van bestanden, webmail, evt. verouderde programmatuur, privé-wifi e.d.) mogelijk leidt tot extra kwetsbaarheden op beveiligingsgebied, is het dringende advies om primair de tooling en middelen te gebruiken die de organisatie je aanbiedt, zeker als je werkt met vertrouwelijk informatie.

Ook als je thuiswerkt heb je een verantwoordelijkheid op het gebied van vertrouwelijke gegevens. Door het implementeren van onderstaande checklist kun je aan deze verantwoordelijkheid invulling geven.

Checklist Veilig Thuiswerken

1. Stel de juiste basisinstellingen voor veiligheid en privacy in op al je middelen in je thuiswerk-situatie (laptop, computer, printer, telefoon, enz.). Wanneer je twijfelt, lees de handleiding van het apparaat of neem contact op met de helpdesk.
2. Zakelijk
   - Zorg goed voor je apparatuur en maak een veilige verbinding met internet (geen openbare verbinding zonder wachtwoord);
   - Bewaak de actualiteit van je hard- en software (dus installeer aangeboden updates zo snel mogelijk), i.v.m. de support van de leverancier;
   - Gebruik alleen vertrouwde draadloze netwerken;
   - Beveilig je draadloze netwerk met een veilig en sterk wachtwoord;
   - Update het besturingssysteem en de software op je apparatuur zeer regelmatig;
   - Gebruik voor je zakelijke activiteiten altijd je virtuele werkplek binnen de Citrix-omgeving, ook als je thuiswerkt (of managed laptop, VPN en andere MFA oplossingen);
   - Gebruik liefst een veilige app Signal of Threema i.p.v. WhatsApp, zeker als het gaat om het delen van zeer vertrouwelijke informatie;
   - Gebruik een wachtwoordenkluis.
3. Werk je op een apparaat van jezelf?
   - Installeer alle software updates direct;
   - Gebruik een goede virusscanner;
   - Verwijder eventueel lokaal opgeslagen werkinformatie onmiddellijk na gebruik (ook uit de prullenbak!);
   - Mailen naar je privé account is niet toegestaan.
4. Privé
   - Zet op al je privé-accounts tweefactor-authenticatie, denk aan Twitter, Facebook, Whatsapp, Gmail, Signal, Linked-in, enz. en check geregeld of je wachtwoorden zijn gelekt (bijv. op de website Scattered Secrets).
5. Je werkruimte
   - Werk thuis volgens het clean desk principe: sluit je computer na gebruik af, laat geen documenten liggen. Vergrendel ook thuis het scherm als je weggaat van de werkplek;
   - Zorg ervoor dat je de werkruimte goed opruimt, weet wat je wel en niet kunt bespreken als er mensen op gehoorafstand zijn. Bespreek vertrouwelijke informatie alleen in een afgesloten ruimte;
   - Moet je echt iets printen? Gooi deze documenten na gebruik dan niet zomaar weg maar versnipper ze eerst. Of bewaar ze op een veilige plaats thuis en gooi later weg op kantoor;
   - Deel bedrijfsapparatuur nooit met familie of vrienden/bekenden. Laat hen niet meelezen op het scherm;
   - Wees voorzichtig met het plaatsen van foto's van je thuiswerkplek/apparatuur op sociale media. Wees bewust van informatie die op de foto in te zien is.
6. Wees alert op verdachte contacten via telefoon, sms, e-mail en sociale media.
   - Open geen bijlagen, klik niet op links en vul geen gegevens in, als je de afzender niet kent of vertrouwt. Dit geldt ook voor SMS- en Whatsapp-berichten en telefoontjes;
   - Verifieer of een onbekende persoon daadwerkelijk is wie hij/zij zegt te zijn (check bijvoorbeeld het e-mailadres van de afzender;
   - Verstrek nooit vertrouwelijke gegevens aan onbekenden;
   - Meld berichten die je niet vertrouwt. Je service-desk kan je waarschijnlijk helpen.
7. Gebruik alleen een video-vergader toepassing die door je werkgever is goedgekeurd. Niet alle programma's voldoen aan de eisen van privacybescherming en informatiebeveiliging.