Auteurs: Maurice Derogee is werkzaam als Information Security Officer bij servicepunt71.
Maurice is bereikbaar via m.derogee@servicepunt71.nl

Thuiswerken in (post)coronatijd

We zijn alweer een nieuw jaar gestart en nog volop bezig met dat waarmee wij het afgelopen jaar afsloten: het coronavirus. Terugkijkend op (voor mij) thuiswerken sinds 12 maart 2020 als informatiebeveiliger, voelt het toch wel als een tropenjaar met vele gezichten en gemengde gevoelens. De titel van dit artikel waarin (post)corona staat vermeld, schrijf ik in december 2020 waarbij ik vurig hoop op het weg kunnen halen van deze haakjes maar, eigenlijk weet ik wel beter.

Wat is mij nou eigenlijk opgevallen aan het thuiswerken in het afgelopen jaar? Nu ik mij dat zo afvraag, gaan de raderen draaien en constateer ik (vanuit mijn werkveld) dat op het gebied van incidenten en datalekken het relatief stil is gebleven. En de cijfers liegen er toch weer niet om, die de AP publiceert omtrent datalekken. Achterdochtig denk ik dan: 'zouden de mensen dat dan wel netjes hebben gemeld als deze gebeurtenissen hen overkomen waren', immers thuis werk je op jouw eigen manier en tijdstippen; is er geen groep collega's die met jou de ruimte delen en zijdelings meekrijgen wat je uitvoert, lees: de sociale controle. Al zit je enkel in je overhemd met daaronder de boxershort in een video meeting, niemand zal het weten. En als beveiliger is het 'niet weten' iets waar je van wakker kan liggen en dan doel ik niet op de (in)correcte kleding van de collega's in de meeting, maar natuurlijk wat deze zo allemaal uitvoeren en of dit dan binnen onze kaders regeltjes en beleid past.

Zou ik het weten als dit niet zo was? "Een goede vraag, niet!" Gelukkig kan ik voor mijn werkveld zeggen dat ik binnen de organisatie in ieder geval een basis heb van werkplekken die hetzelfde zijn ingericht en beveiligd alsook nog centraal kunnen worden beheerd via een Mobile Device Management oplossing. Kunnen schrijf ik bewust want daarop lopen we nog achter. De e-mails worden automatisch gescand op phishing, malware, virussen, spam en de geldende e-mailstandaards (vanuit het forum standaardisatie). Voor het versturen van gevoelige zaken hebben we een voor ons goed werkend systeem ingericht met - in onze e-mail client - een plug-in die ook meeleest en jou wijst op gevoelige inhoud of de onbekende geadresseerde waarheen je deze gegevens wilt gaan sturen.
De systemen zelf zijn voorzien van goed werkende lokale beveiliging welke vanuit de cloudomgeving worden beheerd. Dat geeft wel rust en zeker met een SOC-service die goed op de hoogte is van onze omgeving, de crown jewels en dit voor ons 7x24x365 dagen bewaakt. Hieraan een escalatiematrix voor de handelingen die zij mogen verrichten in overleg met onze externe partners (want we hebben een outsourcing achter de rug dus nu meer dan drie externe partijen die alles doen).
Achterover leunen dus, zou je zo denken, helaas zo werkt het niet. De security patches vliegen om de oren en de phishingmails worden niet allemaal tegengehouden. Hier en daar wat miscommunicatie met de beheerorganisatie, waardoor belangrijke zaken (te) lang bleven liggen. Ook kom je tot de conclusie dat de werkplekken toch best veel vrijheden bieden en dus mensen allerhande apps proberen te installeren zoals Zoom, Jitsi, Google Hangouts en wat nog meer; dus beleid aanpassen, een standpunt innemen en tegelijk de antivirus applicatie aanpassen want wij willen enkel Teams als standaard. Inderdaad MS Teams, maar we zitten nu eenmaal in de 365 cloud en hebben hier kennis van en ondersteuning voor, en niet de mogelijkheid allerlei alternatieven te onderzoeken (op afstand).

Nu werken onze werkplekken buiten het kantoor ook nog via een VPN om binnen bij de bedrijfsomgeving te komen en gebruiken we de Office365 omgeving van Microsoft met als extra MFA. Wacht even? MFA?, dan moeten we een app installeren op de zakelijke smartphone maar die worden (nog) niet beheerd. Dan zenden we wel een handleiding naar onze medewerkers en dan komt alles goed?!
Ik besef echter dat met de praktische oplossing die zakelijke telefoon dus ook de Achilleshiel vormt van onze werkplekbeveiliging. Aan de telefoon zit geen beleid gekoppeld, geen specifieke beveiliging en de medewerkers zelf doen er werkelijk alles mee. En terwijl ik dit schrijf komt er een melding via e-mail van een mogelijk incident op een zakelijke telefoon binnen.

Ondanks de 5 graden buiten heb ik het warm gekregen, begint mijn onderzoek en gelukkig blijkt al snel dat het loos alarm is, want de vreemde codes en gekke nummers - waar deze vandaan gekomen zijn - betroffen de MFA-codes per SMS. Dan nog maar even een uitleg het intranet opsturen. Weer een nieuw bericht; dit keer van de IBD over gevallen van WhatsAppfraude waarbij criminelen met de 6-cijferige code - bedoeld voor overzetten van jouw account naar een nieuwe telefoon - het account kunnen overnemen. Dus weer een nieuw intranetbericht, nu om mensen te waarschuwen, te instrueren hoe te handelen en ook indien het al is misgegaan. Gelukkig geen meldingen (althans voor zover ik weet).

Ondertussen nog een Coordinated Vulnerability Disclosure (Responsible Disclosure) melding van een oplettende burger dat er een FTP-server kwetsbaar is op het SMB-protocol dus meteen hem bedanken en dat ook weer intern doorzetten zodat het verholpen kan worden. Eigenlijk business as usual, valt mij zo op, maar dan alleen vanuit huis met regelmatig de behoefte zaken direct met betrokkenen te bespreken zonder naar een scherm te praten. Want je merkt toch wel dat dit vaak een beter effect heeft en het

doel eerder wordt bereikt dan via videobellen.
Al met al toch weer dezelfde conclusies als ook in de diverse oefeningen vanuit het Rijk in oktober 2020 tijdens de Overheidsbrede Cyberoefening. Weet wat je hebt, wat hiervan extra belangrijk is en zorg dat dit up-to-date blijft. Niet meer te patchen, maak dan werk van het vervangen of uitfaseren. Kan dat echt niet, probeer dit dan te isoleren van de rest van de systemen (segmentatie). Monitoring en logging zijn van groot belang alsook wie er (waarvoor) verantwoordelijk is binnen de organisatie en hoe er ook op afstand een team kan worden samengesteld (CSIRT) bij een incident of calamiteit.

Een SOC service is van grote toegevoegde waarde, helemaal als zij de firewalls beheren en kwetsbaarheden in kaart brengen. Naast de juiste personen intern natuurlijk ook extern - als er geoutsourced is met de juiste bevoegdheden - want je wilt spijkers met koppen slaan als het nodig is.
En als laatste punt maar feitelijk als belangrijkste eerste punt het bewustzijn van de medewerkers. Naast oefenen, oefenen, is ook trainen noodzakelijk. Gooi die PowerPoint nu eens weg en zoek naar een oplossing waar je kunt bijhouden hoe de adoptie is van de uitgestuurde trainingen en ook de diversiteit aan onderwerpen. Hou het vooral leuk en afwisselend. Maar vergis je niet, want zo een awareness tool - zou je er al eentje mogen aanschaffen of al hebben - is een hele klus. Net zoals beleid moet het aansluiten bij de organisatie, de werkzaamheden per afdeling, de missie, visie en strategie van de organisatie. Last but not least, moet het ook nog eens te begrijpen zijn. Maar naast dit alles, nog een niet onbelangrijk aspect: de werkplekken én daar versta ik dan ook de telefoon onder. Deze moeten echt wel beheerd zijn, want denk maar aan een gebouw of 40 met (voor mij) 2.500 onbeheerde deuren naar binnen en nog eens 2.500 onbekende locaties erbij als je het thuiswerken meeneemt. Kan dit ook met BYOD ofwel iedereen gebruikt eigen apparatuur, al dan niet via een budget vanuit de werkgever?

Ja, dat kan zeker wel, maar ook hier zul je dan als werkgever een beleid voor moeten opstellen met behulp van de beveiligingsorganisatie. De medewerker daarbij volledig vrijlaten met betrekking tot de wijze waarop verbinding wordt gemaakt met welk apparaat van zijn keuze dan ook. Daarbij stelt de verbindingsprogrammatuur zelf de eisen waaraan het apparaat dient te voldoen om verbinding te mogen maken (verbindingsregels: profiling). Dat, alhoewel ik hier zelf geen voorstander van ben (denk aan een realisatie binnen de traditionele Citrix-omgevingen).

Ik ben wellicht wat traditioneel, maar mijns inziens moet een zakelijke omgeving met beheerde apparatuur worden benaderd en dat zeer zeker bij een organisatie die tot de overheid behoort of gevoelige gegevens van cliënten beheert. Dat kan op diverse manieren en er is altijd wel een passende oplossing denkbaar waarbij ook de medewerker tevreden kan zijn met de door de werkgever verstrekte middelen of keuzes.

Het CYOD oftewel Choose Your Own Device biedt mogelijkheden van keuzevrijheid onder voorwaarde van beheerde en beheersbare werkplekken. Ik zie al jaren discussies over de diverse scenario's en allemaal bezitten ze zowel voor- als nadelen. Het hangt vooral van het soort organisatie af. Echter, zoals zo vaak geroepen wordt en wat ik als een waarheid beschouw, dichtspijkeren is niet de weg.
Zakelijke apparatuur, zoals de smartphone, kan worden voorzien van een gewenst privé profiel; zodat je ook een eigen omgeving kunt realiseren met de foto van het gezin op de achtergrond. Als beheerder geef je dan precies aan wat er wel en niet tussen de profielen mag worden uitgewisseld. En voor de werkplek is het een vraag of die persoonlijke achtergrond echt wel zo erg is, want je kunt ook afspreken dat bij gesprekken met klanten - via bijvoorbeeld Teams - een zakelijke achtergrond wordt gebruikt met de bedrijfshuisstijl.

En verbied je de installatie van applicaties uit de Microsoft Appstore of Google Play, zorg er dan wel voor dat alle tools en applicaties die nodig zijn er al op staan of heel snel kunnen worden beoordeeld en geleverd op afstand! Langskomen op de zaak voor zoiets, is inmiddels toch zó 2019. En denk ook na over randapparatuur die thuis kunnen worden gekoppeld - zoals privéprinters en externe harddisks of ander soortige opslagmedia - want daar word je zeker mee geconfronteerd als je een werkplek beheert en uitgeeft. Laat vooral een diverse groep collega's in een pilot het werkplek-concept goed testen, zorg ervoor dat er een goed programma is opgezet voor de adoptie van het concept alsook alle tools en applicaties die er worden meegeleverd.

Wat mij in de coronacrisis vooral is opgevallen is dat mensen door alle maatregelen zich bewuster zijn geworden van de diverse risico's en dat er voor ons als beveiligers toch een soort van rode loper is uitgerold, omdat veel van ons werk hier direct naartoe te vertalen is. Mensen begrijpen de door ons geschetste risico's nu beter dan voorheen. Laten wij beveiligers die kans grijpen!