Intro Alwin
Ik ben Alwin Zegers, in dienst bij VNG sinds 2012 en ook werkzaam bij het team Informatisering & Automatisering. In mijn dagelijkse werkzaamheden veel betrokken bij de ICT dienstverlener vanwege het doorvoeren van changes, troubleshooten van incidenten en het initiëren van nieuwe ontwikkelingen (waarbij ook vaak als projectleider optreedt). Een belangrijk aandachtsgebied voor mij vormt de ICT veiligheid, vandaar dat ik jullie hier wat meer over zal vertellen.

iBewustzijn
Nieuwe medewerkers zijn verplicht om een iBewustzijn cursus te volgen bij de VNG waarbij we inzoomen op belangrijke zaken als phishing, datalekken melden etc. Om het bewustzijn actief te houden en onze procedures te testen, zorgen we ook af en toe voor incidenten in de vorm van een nep-phishing mail of hack-aanval. We zien dat hierdoor het bewustzijn vergroot wordt en er meer vragen gesteld worden, maar we hebben het nog zeker niet voor elkaar dat niemand op een phishing link klikt.

Pentesten
Ons uitgangspunt is dat systemen zoveel mogelijk bijgewerkt zijn en voldoen aan de laatste stand van de techniek. Om dit te verifiëren, organiseren we regelmatig een pentest voor websites, maar bijvoorbeeld ook voor het netwerk, zodat we ons ook bewust worden van eventuele omissies in de veiligheid en hier verdere actie op kunnen nemen en onze leveranciers scherp kunnen houden.

BIO – IBD
In ons gebouw is ook de IBD aanwezig. Zij vormen een centrale dienst voor gemeenten op het gebied van informatieveiligheid. VNG is hierbij ook aangesloten, zodat we informatie vanuit de IBD krijgen over belangrijke lekken. De IBD heeft voor gemeenten de BIO richtlijn opgesteld. Deze vormt voor ons een richtlijn op het gebied van informatieveiligheid, alhoewel we natuurlijk geen gemeente zijn en bijvoorbeeld geen gegevens over burgers registreren of paspoorten uitgeven.

Uitfasering Kaspersky
Naast het volgen van richtlijnen hebben wij ook te maken met verdere ontwikkelingen in de wereld. Zo hebben wij ook enkele internationale bedrijven in ons pand, en wanneer die meedoen aan biedingen op

projecten kunnen we eisen krijgen zoals bijvoorbeeld een verbod op de virusscanner Kaspersky op onze systemen. Het afgelopen jaar is VNG dan ook bezig geweest om over te stappen op Defender for Endpoint.

VNG-laptops beheert via Intune
Voor onze vaste medewerkers bieden wij een door Intune beheerde Windows 11 laptop aan. Door het beheer vanuit Intune te doen en ons zoveel mogelijk aan door Microsoft aanbevolen richtlijnen te voldoen, is het beheer van onze laptops een stuk eenvoudiger geworden.
Op enkele uitzonderingen na, zijn medewerkers geen lokaal beheerder op de laptop.

SSO & Conditional Access & BYOD
Voor al onze webapplicaties vereisen wij SSO om in te kunnen loggen. MFA is hierbij altijd verplicht, en door middel van Conditional Access dwingen wij diverse zaken af om de accounts zo maximaal mogelijk te beveiligen. VNG heeft een BYOD-beleid waarbij we iedereen toestaan de eigen laptop en telefoon te gebruiken. Mede hierdoor hebben we ook Mobile Application Management ingericht. Mobile Device Management wordt niet toegepast.

MS Secure Score
Voor een indicatie van onze veiligheid hebben we ook een plaatje van onze secure score toegevoegd. Hierbij willen we opmerken dat wij deze score niet handmatig bijwerken, dus we handelen punten niet af met de opmerking dat wij het risico accepteren of het probleem op een andere manier hebben opgelost.