Reactie 1e termijn:

Zelfs zoveel maanden later is het gevoel bij dit Rekenkamerrapport intens. Door het inzetten van een hacker heeft de Rekenkamer op een innovatieve manier een onderzoek gepleegd, dat ons ruw wakker heeft geschud:

(PvdA) De hele ontwikkeling rondom BLOU heeft er voor de gemeente Oss voor gezorgd dat er te lang niet is geïnvesteerd in de langere termijn. Dat heeft er toe geleid dat we in 2019 een enorme inhaalslag hebben gemaakt. Ja we waren al bezig met informatieveiligheid, ja we hadden processen, ja we hadden een functionaris, maar in de praktijk bleek dat we ondanks het feit dat we dachten dat we op orde waren op geen enkele manier beschermd waren tegen moedwillige inbreuken. De boodschap is hard geland.
Het rekenkamer onderzoek kwam op een moment dat we volop in de verbeterslag en implementatiefase zaten van veel nieuwe systemen. Dat heeft er enerzijds voor gezorgd dat we op dat moment erg kwetsbaar waren maar heeft er direct daarna voor gezorgd dat we de tegenmaatregelen snel konden treffen. Dat heeft onder andere geresulteerd in snelle overgang naar VDI vanuit Citrix en een stabiel netwerk voor alle thuiswerkende collega's tijdens de coronacrisis. De cryptische omschrijving is terug te leiden naar het feit dat we niets in het openbaar prijs willen geven van onze tegenmaatregelen. Dit zou namelijk weer een opening kunnen zijn voor 'echte' hackers en dat willen we voorkomen.

Het spreekt voor zich dat wij duurzame aandacht voor informatieveiligheid willen (SP). Dit rekenkameronderzoek zal nog lang naijlen. Informatieveiligheid heeft onze hoogste prioriteit. (SP,GL) We hebben voor ICT extra formatie aangevraagd en ook gekregen. Dit is onder andere nodig om informatieveiligheid te verbeteren. Hier komt 1 Fte extra voor beschikbaar. (PvdA)

Zelfs in tijden van een coronacrisis blijven hackers actief en moeten we onze informatie optimaal beschermen. Informatieveiligheid is niet statisch maar een doorlopend proces. Binnen ICT zijn daarvoor al de nodige aanpassingen gedaan in de communicatiestructuren. Informatieveiligheid heeft een eigen team met experts met daarbij een duidelijke escalatieprocedure bij dreiging. Er is voorheen onvoldoende aandacht geweest voor structurele inzet van hackers en overige testen op het netwerk. Dit gebeurde wel maar vooral adhoc. Om alle activiteiten in samenhang te brengen is nog meer inzet vanuit ICT nodig. Hiervoor is budget aangevraagd in de Marap.

Vanuit het onderzoek van rekenkamercommissie is toegezegd dat er een hertest wordt uitgevoerd. Om informatieveiligheid echter in een Plan-Do-Check-Act cyclus te krijgen is een structurele aanpak vereist. Dit betekent periodiek hertesten door externen in een brede context, niet alleen technisch maar ook op gebied van bewustzijn van onze medewerkers. Hiervoor is in de Marap budget aangevraagd

De hertest is gepland in de maand april en mei. Door de enorme druk op de ICT door de coronacrisis is dit verdeeld over 2 maanden. Het is doel van de hertest is om het lerende effect te vergroten. Op basis van het eerder uitgevoerde onderzoek door DongIT worden nu de uitgevoerde

tegenmaatregelen getoetst (D66) door die zelfde organisatie (extern GL). De technische bevindingen die zijn gedaan door de hacker zijn direct omgezet in verbetermaatregelen. Deze acties worden in de hertest opnieuw getoetst. (D66) Uiteraard kunnen we die bevindingen en de structurele aanpak rondom informatieveiligheid toelichten. De vorm waarop de terugkoppeling plaatsvindt is afhankelijk van het verloop van de coronacrisis, dit gaat waarschijnlijk niet lukken voor de zomer van 2020. (VDG) Echter: Periodiek rapporteren is onderdeel van de plan-do-check-act cyclus en wordt vast onderdeel van de bedrijfsvoering van ICT

Er is mede naar aanleiding van het rekenkamer onderzoek een communicatiecampagne opgezet. De campagne 'Veiligheid' bestaat uit diverse onderdelen. In de campagne laten we zien wat we van medewerkers verwachten zodat we veilig kunnen werken. (CDA) We leggen goed uit waarom en we gebruiken één overkoepelend beeld en één centrale boodschap bij alle berichten. Het communicatiedoel van alle onderdelen is gedragsverandering. We maken voor de campagne drie thema's, met bijna dezelfde titel en opmaak:

- Veilig aan het werk
- Veilig op het werk
- Veilig naar je werk

Enkele concrete voorbeelden van gedragsmaatregelen die we gaan uitwerken in de campagne 'Veiligheid';

- Laat je pas zien als je het gemeentehuis binnenkomt.
- Laat je pas niet slingeren
- Laat niemand meekijken op jouw scherm
- Sluit je scherm af wanneer je wegloopt van je werkplek
- Is je brief in Klare taal? Haal de persoonsgegevens eruit.

Bij alle communicatie gebruiken we een van deze drie logo's en huisstijl. We zorgen voor meetbare activiteiten waarop we kunnen blijven rapporteren. Raadsleden zijn onderdeel van deze campagne Veiligheid. (VVD)