Memo aan de Raad van Bestuur
Onderwerp: Assumptions & Missing Info bij risicoscoring Vanguard Health
Datum: 16-02-2026
Van: Viresh Sheoratan en Muazma Anwar

Geachte Raad van Bestuur, Voor het risicoregister (12 risico's) hebben wij een eerste scoring gemaakt. De hoogste risico's zijn: R1 phishing, R2 accountmisbruik door beperkte extra inlogbeveiliging, en R11 onveilige netwerkinstellingen. Om de scoring definitief te maken, missen wij nog informatie die nodig is voor een betrouwbare beoordeling van continuïteit en patiëntveiligheid.

1) Welke info missen wij?
- Inlogbeveiliging (MFA): waar wel/niet verplicht, per systeem en gebruikersgroep.
- Accountbeheer: hoe snel accounts worden verwijderd bij uitdienst/stage-einde.
- Autorisaties: hoe vaak rechten op EZPD, DLO, VPN en beheeraccounts worden gecontroleerd.
- Monitoring: of beveiligingscontrole 24/7 actief is (ook avonden/nachten/weekenden).
- Back-up en herstel: of restoretests recent zijn uitgevoerd en wat de uitkomsten waren.

2) Welke vragen stellen wij aan Vanguard Health?
- Waar is extra inlogbeveiliging nu verplicht, en waar nog niet?
- Binnen hoeveel tijd worden oude accounts verwijderd?
- Hoe vaak worden toegangsrechten herzien?
- Is monitoring en opvolging van verdachte activiteiten 24/7 geregeld?
- Wat zijn de resultaten van de laatste back-up/restoretest?

3) Welke aannames beïnvloeden onze scoring?
- A1: Extra inlogbeveiliging staat nog niet overal aan → verhoogt kans op R1 en R2.
- A2: Oude accounts worden soms te laat verwijderd → verhoogt kans op ongewenste toegang.
- A3: Netwerk is niet overal goed gescheiden → verhoogt impact van aanvallen.

Kort verzoek
Wij vragen akkoord om deze informatie op te halen bij IT, Security, HR en leveranciers. Na ontvangst herijken wij binnen de scores en leveren wij een definitieve risicomatrix met prioriteiten. Met vriendelijke groet, Viresh Sheoratan en Muazma Anwar AD Cybersecurity