METRIC-IT

10 KRITISCHE VRAGEN OVER HET ZORGNETWERK

Is **jouw netwerkinfrastructuur** klaar voor veilige, continu beschikbare zorg?

Digitale zorgprocessen zijn volledig afhankelijk van een stabiele en veilige netwerkinfrastructuur. Van patiëntendossiers en medische apparatuur tot mobiele zorgapplicaties: alles draait op connectiviteit.

Tegelijkertijd nemen de eisen aan zorgnetwerken snel toe. Nieuwe regelgeving zoals NIS2 en NEN 7510, een groeiend aantal verbonden apparaten en steeds mobieler zorgpersoneel maken het netwerk complexer dan ooit. Toch wordt een netwerk nog te vaak beoordeeld op basis van prestaties van vandaag, terwijl continuïteit, veiligheid en schaalbaarheid juist in het ontwerp besloten liggen.

Daarom hebben we de 10 belangrijkste vragen verzameld die bestuurders, IT-managers en securityverantwoordelijken zichzelf zouden moeten stellen over hun zorgnetwerk. Geen technische checklist, maar strategische vragen die **inzicht geven in de weerbaarheid, schaalbaarheid en betrouwbaarheid van je netwerkinfrastructuur.**

1.

Hoe ontwerp ik een toekomstbestendig wifi-netwerk in een complexe zorgomgeving?

Een stabiel zorgnetwerk begint niet bij access points, maar bij het ontwerp. In een zorgomgeving beïnvloeden bouwkundige constructies, medische apparatuur en mobiliteit continu de wifi-signalen. Een professioneel uitgevoerde meting vormt de basis. Ontwerp op basis van meetdata, back-up en capaciteit, niet op aannames. Stabiliteit ontstaat in de ontwerpfase. Niet wanneer gebruikers al klachten melden.

2.

Is mijn zorgnetwerk berekend op piekbelasting en kritische zorgmomenten?

Zorgnetwerken falen niet bij gemiddeld gebruik, maar tijdens piekmomenten. Denk aan momenten waarop veel apparaten tegelijk inloggen, zorgpersoneel massaal apps gebruikt of cruciale gegevens worden overgedragen. Capaciteit moet vooraf worden doorgerekend op basis van worst-case scenario's. Wie alleen ontwerpt op gemiddelde belasting accepteert risico op procesverstoring. Continuïteit begint bij het juist afstemmen van capaciteit en ontwerp.

Stabiliteit begint bij ontwerp, niet gebruik

3.

Kan mijn zorgnetwerk-gebruikers verbinden zonder onderbreking, zelfs wanneer ze zich verplaatsen?

In de zorg is mobiliteit geen luxe, maar een essentieel onderdeel van het zorgproces. Apparaten moeten naadloos verbinding houden, zonder dat telefoongesprekken, toegang tot patiëntendossiers of apps worden onderbroken. Dit vraagt om een goed afgestemd netwerk en duidelijke regels voor wie toegang heeft en hoe snel gegevens worden verwerkt. Als het overschakelen van verbindingen niet getest is, blijft het een aanname en dat kan risico's geven voor de continuïteit binnen de zorg.

4.

Hoe kan ik ervoor zorgen dat patiëntgegevens gescheiden worden van ander netwerkverkeer?

Het scheiden van netwerken in de zorg draait niet alleen om prestaties, maar vooral om het beheersen van risico's. Medische apparatuur, IoT, kantoorapparatuur en gastennetwerken moeten logisch en technisch gescheiden zijn, met duidelijke toegangsregels en voortdurende monitoring. Een goede indeling voorkomt dat problemen zich makkelijk verspreiden en verkleint de impact op de veiligheid van patiënten. Het inrichten van je netwerk is daarom niet alleen een technische keuze, maar ook een beslissing die governance en beleid raakt.

Continuïteit en veiligheid bepalen zorgnetwerken

5.

Is mijn zorgnetwerk schaalbaar bij uitbreiding of fusie?

Zorginstellingen veranderen continu. Denk aan verbouwingen, tijdelijke units, samenwerkingen en fusies. Een zorgnetwerk is schaalbaar wanneer nieuwe afdelingen, tijdelijke zorgunits of extra locaties eenvoudig kunnen worden toegevoegd zonder dat de basis aangepast hoeft te worden. Dat begint bij een duidelijk en goed opgebouwd netwerkontwerp. Wanneer uitbreiding betekent dat je het netwerk opnieuw moet ontwerpen, ontbreekt schaalbaarheid in de basis. Toekomstbestendigheid **wordt vooraf ontworpen en niet achteraf opgelost.**

6.

Hoe weerbaar is mijn netwerk tegen ransomware zonder zorgprocessen stil te leggen?

Ransomware is geen kwestie van of, maar wanneer je ermee te maken krijgt. Weerbaarheid betekent dat het netwerk slim is ingericht: systemen zijn gescheiden, alleen de juiste mensen hebben toegang en verdachte activiteiten worden snel ontdekt. Maar minstens zo belangrijk is de vraag: hoe snel kun je problemen isoleren zonder dat belangrijke zorgsystemen uitvallen? **In de zorg draait cyberweerbaarheid niet alleen om voorkomen, maar om continuïteit.**

Toekomstbestendig is schaalbaar én weerbaar

7.

Hoe krijg ik 24 uur per dag inzicht in wie er op mijn kritische zorgnetwerk actief is?

Dit begint met een zero-trust-aanpak. Toegang tot het netwerk wordt daarbij gebaseerd op identiteit, rol en context van de gebruiker: binnen én buiten de zorginstelling. Zo voorkom je dat onbevoegden ongemerkt toegang krijgen tot systemen met privacygevoelige patiëntinformatie. **Continu inzicht is essentieel om risico's tijdig te detecteren.**

8.

Voldoet mijn zorgnetwerk aantoonbaar aan de NIS2- en NEN 7510-regelgeving?

Je zorgnetwerk voldoet aantoonbaar aan deze normen wanneer je niet alleen de juiste maatregelen hebt, maar ook kunt laten zien hoe security en beheer structureel zijn ingericht. NIS2 en NEN 7510 vragen om aantoonbaarheid, niet alleen intentie. Compliancy is daarom geen checklist, maar een structurele manier van werken in processen en techniek. Denk aan registratie van activiteiten, toegangsbeheer, gescheiden netwerkzones, continue controle en aantoonbare beheersing van risico's. **De vraag is niet alleen of je voldoet, maar of je dit kunt onderbouwen.**

Compliance vraagt bewijs, geen intentie

9.

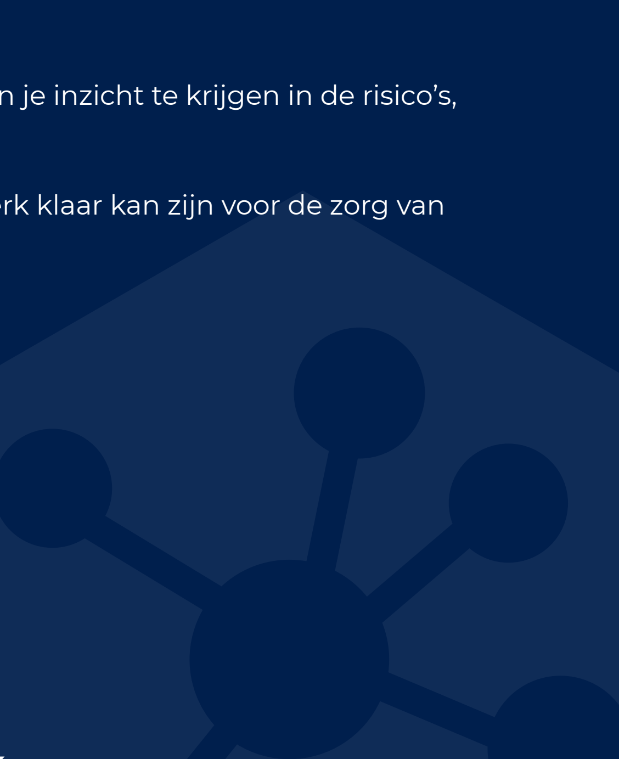
Hoe borg ik netwerkcontinuïteit bij een cyberincident of uitval?

Wanneer het netwerk uitvalt, staat de zorg stil. Back-upverbindingen, automatische overschakeling en gescheiden netwerken zorgen ervoor dat kritieke zorgprocessen kunnen blijven functioneren. Maar een back-up die nooit getest is, geeft slechts een gevoel van zekerheid. **Continuïteit vraagt om regelmatige controles en realistische tests van noodscenario's.**

10.

Hoe hou ik controle over wie er toegang heeft tot patiëntgegevens?

Zonder continu inzicht in je netwerk weet je niet wie of wat verbinding maakt met systemen met gevoelige patiëntinformatie. Door het netwerk 24/7 te monitoren en afwijkend gedrag direct te signaleren, kan ongeautoriseerde toegang vroegtijdig worden ontdekt. Vroegtijdige signalering beschermt niet alleen patiëntgegevens, maar voorkomt ook dat kritieke zorgprocessen stilvallen. **Zichtbaarheid is de basis van privacybescherming en veilige zorg.**



HOE TOEKOMST-BESTENDIG IS JOUW ZORGNETWERK?

Veel organisaties gaan ervan uit dat hun netwerk goed functioneert, totdat er een storing, cyberincident of capaciteitsprobleem ontstaat.

Wil je weten hoe jouw netwerkinfrastructuur ervoor staat?

Onze netwerkspecialisten kijken graag met je mee en helpen je inzicht te krijgen in de risico's, verbeterpunten en groeimogelijkheden van je netwerk.

Neem contact op met METRIC-IT en ontdek hoe jouw netwerk klaar kan zijn voor de zorg van morgen.

Krijg inzicht in je netwerk

METRIC-IT
EMPOWER YOUR NETWORK

De Wel 2J | 3871 MV Hoevelaken | **E:** info@metric-it.nl | **T:** 085 620 2130 | Volg ons op in