KNNS

knns.nl

Digitale gezondheid in het MKB

Trendrapport | 2026

Inhoud

Voorwoord

Digitale gezondheid als bedrijfsrisico

De digitale gezondheid van het MKB wordt in de praktijk steeds zichtbaarder als een bedrijfsrisico. Niet alleen door cyberincidenten zoals ransomware, maar ook door de manier waarop organisaties omgaan met hun digitale basis.

De kwetsbaarheid wordt steeds zichtbaarder. Waar vroeger een verstoring vooral lokaal bleef, zien we nu dat één incident direct impact heeft op meerdere partijen in de keten. Tegelijkertijd groeit de afhankelijkheid van digitale processen, waardoor stilstand sneller ontstaat en langer doorwerkt.

De sector zit daarmee in een overgang. Initiatieven zoals digiGO en standaarden zoals ISO 19650 bieden richting en structuur, maar maken ook duidelijk dat technologie alleen niet voldoende is. Het vraagt om afspraken, regie en een andere manier van samenwerken.

Voor veel organisaties betekent dit dat digitale continuïteit geen IT-vraagstuk meer is, maar een integraal onderdeel van projectbeheersing en risicomanagement.

In dit trendrapport delen onze experts drie inzichten die we in de praktijk steeds vaker terugzien, aangevuld met ontwikkelingen die deze beweging versnellen.

Dennis Wennekers, Technisch Business Consultant KNNS

Digitale gezondheid begint bij de basis en daar gaat het vaak mis

Inzicht 1

Digitale gezondheid begint de basis en daar gaat het vaak mis

Ransomware en accountovernames blijven de meest voorkomende oorzaken van incidenten. Opvallend is dat deze aanvallen zelfden gebruikmaken van geavanceerde technieken. In de meeste gevallen gaat het om bekende kwetsbaarheden of onvoldoende beveiligde accounts.

Dat maakt dit inzicht confronterend. De grootste risico's zitten niet in complexe dreigingen, maar in het niet op orde hebben van de basis. We zien daarbij duidelijke verschillen binnen het MKB. Grotere organisaties nemen vaker meerdere maatregelen tegelijk, terwijl kleinere organisaties blijven hangen in losse oplossingen. Juist dat "stapelen" van maatregelen maakt het verschil.

Organisaties die digitaal gezond zijn, hebben een duidelijke baseline ingericht:

- structureel patchmanagement
- sterke authenticatie zoals MFA
- betrouwbare back-ups
- inzicht via logging en monitoring
- en een periodieke risicoanalyse

Het belangrijkste verschil zit in hoe dit wordt benaderd. Niet als IT-project, maar als randvoorwaarde voor de continuïteit van het bedrijf.

2 Digitale gezondheid verschuift van IT naar de directietafel

Inzicht 2

Digitale gezondheid verschuift van IT naar de directietafel

Waar cybersecurity vroeger vooral een technische verantwoordelijkheid was, verschuift dat steeds meer naar het bestuur. Regelgeving zoals NIS2 maakt dat expliciet.

De kern van die ontwikkeling is simpel: organisaties zijn zelf verantwoordelijk voor hun digitale weerbaarheid. Niet alleen richting hun eigen bedrijfsvoering, maar ook richting klanten, partners en de maatschappij.

Dat heeft directe gevolgen voor hoe organisaties dit organiseren. Het gaat niet meer alleen om tools en maatregelen, maar om:

- risicomanagement
- duidelijke processen voor incidenten
- inzicht in afhankelijkheden van leveranciers
- en bewustwording op directieniveau

In de praktijk zien we dat veel organisaties hier nog in groeien zijn. Governance is vaak impliciet of versnipperd, terwijl de verwachting juist is dat dit expliciet en aantoonbaar wordt ingericht.

Organisaties die hier nu al op voorsorteren, doen dat door NIS2 niet als verplichting te zien, maar als kader om hun digitale organisatie volwassener te maken.

3 Digitalisering versnelt, maar zonder de juiste inrichting vergroot het vooral je risico’s

Inzicht 3

Digitalisering versnelt, maar zonder de juiste inrichting vergroot het vooral je risico’s

Cloud en AI worden steeds toegankelijker en vinden snel hun weg naar het MKB. Dat biedt kansen voor efficiëntie en innovatie, maar brengt ook nieuwe risico’s met zich mee.

We zien dat adoptie vaak sneller gaat dan inrichting. Tools worden geïmplementeerd, maar afspraken over gebruik, toegang en beveiliging blijven achter. Zeker in organisaties waar capaciteit beperkt is, ontstaat daardoor een kwetsbare situatie.

Daarnaast speelt het tekort een ICT-specialisten een grote rol. Veel organisaties hebben simpelweg niet de mensen om digitalisering en beveiliging tegelijk goed te organiseren.

Digitale gezondheid vraagt daarom om een andere aanpak. Niet alleen focussen op technologie, maar op samenhang:

- duidelijke afspraken over toegang en identiteiten
- inzicht in waar data staat en hoe die wordt gebruikt
- logging en monitoring als standaard
- en gerichte ontwikkeling van kennis en vaardigheden

Organisaties die dit combineren, halen waarde uit digitalisering zonder risico’s te vergroten. Organisaties die dat niet doen, lopen het risico dat groei juist leidt tot meer kwetsbaarheid.

Conclusie

Digitale gezondheid als fundament voor continuïteit

Digitale gezondheid in het MKB wordt steeds bepalende voor de continuïteit van organisaties. Niet omdat dreigingen nieuw zijn, maar omdat afhankelijkheid van digitale processen blijft toenemen.

Wat in de praktijk opvalt, is dat de grootste risico's vaak niet in complexe aanvallen zitten, maar in de basis. Tegelijkertijd verschuift e verantwoordelijkheid steeds nadrukkelijker van IT naar de bredere organisatie en het bestuur. Digitalisering gaat door, maar zonder de juiste inrichting leidt die groei eerder tot extra kwetsbaarheid dan tot meer controle.

Voor organisaties betekent dit een duidelijke verandering in perspectief. Digitale gezondheid is geen bijzaak meer of een los IT-schema, maar een structureel onderdeel van de bedrijfsvoering. Het vraagt om samenhang tussen techniek, processen en verantwoordelijkheden.

Organisaties die daar nu bewust op sturen, versterken niet alleen hun weerbaarheid, maar bouwen ook aan vertrouwen richting klanten, partners en de keten als geheel.