KNNS

knns.nl

Digitale continuïteit in bouwbedrijven

Trendrapport | 2026

Inhoud

Voorwoord

Digitale continuïteit als randvoorwaarde

Digitale continuïteit in de bouw staat steeds vaker onder druk. Niet alleen door cyberincidenten zoals ransomware, maar ook door de manier waarop informatie tussen partijen wordt gedeeld. Projecten draaien op data, maar die data is vaak versnipperd over systemen, organisaties en fases.

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 branche-experts drie inzichten die we in de praktijk steeds vaker terugzien, aangevuld met ontwikkelingen die deze beweging versnellen.

Dennis Wennekers, Technisch Business Consultant KNNS

K

Continuïteit faalt zelden door de aanval zelf, maar door wat er daarna gebeurt

Inzicht 1

Continuïteit faalt zelden door de aanval zelf, maar door wat er daarna gebeurt

In discussies over cybersecurity ligt de focus vaak op voorkomen. Hoe houden we aanvallers buiten? In de praktijk blijkt dat de grootste schade juist ontstaat wanneer organisaties niet goed voorbereid zijn op herstel.

Incidenten zijn namelijk niet volledig te voorkomen. Dat is ook de lijn die het NCSC volgt. Het verschil zit in hoe snel en gecontroleerd je weer operationeel bent. En precies daar gaat het in de bouw vaak mis.

Veel organisaties hebben back-ups, maar testen ze zelden. Scenario's zijn bedacht, maar nooit geoefend. En afhankelijkheden van leveranciers of projectomgevingen zijn niet altijd inzichtelijk. Daar zit de echte kwetsbaarheid.

Organisaties die dit goed aanpakken, draaien het perspectief om. Niet alleen beschermen, maar vooral herstellen:

- herstelbaarheid als KPI (bijvoorbeeld RTO en RPO per proces)
- back-ups die echt los staan van de primaire omgeving
- duidelijke eisen aan partners, zoals MFA en segmentatie
- en periodieke crisisoefeningen

Wie dat structureel organiseert, beperkt de impact van incidenten drastisch. Wie dat niet doet, ontdekt het pas als het te laat is.

2 Informatiecontinuïteit is projectcontinuïteit

Inzicht 2

Informatiecontinuïteit is projectcontinuïteit

In de bouw draait alles om informatie. Tekeningen, modellen, planningen, revisies. Als die informatie niet klopt, niet compleet is of niet op het juiste moment beschikbaar is, ontstaat er direct vertraging, rework en discussie.

Toch zien we dat informatiestromen vaak versnipperd zijn. Verschillende definities, verschillende versies, verschillende systemen. Iedereen werkt met data, maar niet altijd met dezelfde waarheid.

Daarom krijgt informatiemanagement steeds meer aandacht. ISO 19650 speelt hierin een belangrijke rol. Niet als theoretisch model, maar als praktisch kader om afspraken te maken over wie welke informatie levert, wanneer die beschikbaar moet zijn en hoe die wordt beheerd.

De kracht zit vooral in het creëren van structuur. Door te werken met een gecontroleerde digitale omgeving (CDE) blijft informatie consistent over de verschillende projectfasen heen en wordt overdracht tussen partijen betrouwbaarder. Dat voorkomt misverstanden en maakt samenwerking efficiënter.

Organisaties die dit goed organiseren, merken dat projecten rustiger verlopen. Faalkosten nemen af, besluitvorming wordt beter onderbouwd en de voorspelbaarheid neemt toe.

De belangrijkste stap is niet technisch, maar organisatorisch: afspraken expliciet maken en vastleggen, en die ook contractueel borgen.

3 De grootste continuïteit-risico zit in de keten, niet binnen één organisatie

Inzicht 3

De grootste continuïteitsrisico zit in de keten, niet binnen één organisatie

De bouw is per definitie een ketensector. Hoofdaannemers, onderaannemers, leveranciers, adviseurs. Allemaal werken ze samen aan hetzelfde project, maar vaak met hun eigen systemen en werkwijzen. Dat is precies waar het schuurt.

Steeds meer bedrijven werken digitaal, maar de samenhang ontbreekt. Systemen sluiten niet goed op elkaar aan, data wordt dubbel vastgelegd of raakt onderweg verloren. En als er ergens iets misgaat, verspreidt dat effect zich snel door de keten. Daarmee wordt ketenfragmentatie een structureel continuïteitsrisico.

De oplossing ligt niet in nóg een systeem, maar in betere aansluiting:

- werken met gedeelde standaarden
- duidelijke uitwisselprofielen en API’s
- en afspraken over security en datagebruik

Initiatieven zoals digiGO en het Digitaal Stelsel Gebouwde Omgeving laten zien dat de sector die kant op beweegt. Maar in de praktijk moeten organisaties hier zelf ook keuzes in maken.

Wie inzet op interoperabiliteit en ketencompatibiliteit, bouwt aan robuustere projecten. Wie dat niet doet, blijft afhankelijk van maatwerk en handmatige oplossingen.

Conclusie

Continuïteit vraagt om regie over de keten

Digitale continuïteit in de bouw gaat allang niet meer alleen over beveiliging. Het draait om het vermogen om te herstellen, om de kwaliteit en beschikbaarheid van informatie en om de manier waarop partijen in de keten samenwerken.

In de praktijk blijkt dat incidenten niet volledig te voorkomen zijn, maar dat de impact ervan sterk wordt bepaald door hoe goed organisaties zijn voorbereid op herstel. Tegelijkertijd wordt duidelijk dat informatiekwaliteit direct invloed heeft op het verloop van projecten. Wanneer data niet klopt of niet beschikbaar is, ontstaat er vertraging en onzekerheid.

Daarbovenop komt de complexiteit van de keten. Bouwprojecten zijn afhankelijk van meerdere partijen die allemaal met eigen systemen en werkwijzen opereren.

Juist in die samenwerking ontstaan de grootste risico's, omdat verstoringen zich snel verspreiden en moeilijk te beheersen zijn.

Voor organisaties betekent dit dat digitale continuïteit breder moet worden benaderd. Niet als een geïsoleerd IT-thema, maar als een integraal onderdeel van projectbeheersing en risicomanagement. Het vraagt om duidelijke afspraken, inzicht in afhankelijkheden en regie over hoe informatie en processen door de keten bewegen.

Organisaties die daar nu bewust op sturen, beperken niet alleen risico's, maar creëren ook meer voorspelbaarheid en controle in een sector die steeds digitaler en complexer wordt.