



# Voorkom bouwvertraging met een veilig en efficiënt netwerk

Ga voor maximale veiligheid op kantoor en op de bouwplaats

# Ga voor maximale veiligheid op kantoor en op de bouwplaats

Bouwen is al heel lang veel meer dan alleen stenen op elkaar plaatsen voor een solide structuur. Zo wordt er bij de opstart van een bouwproject eerst een digitaal netwerk aangelegd dat de cruciale brug vormt tussen het hoofdkantoor en de bouwplaats. Dit netwerk zorgt voor de broodnodige ondersteuning van digitale tools op de bouwplaats. Een efficiënte informatie-uitwisseling tussen het kantoor en de bouwplaats is de kritische succesfactor. Zeker nu de databehoeftte ongekende hoogtes bereikt. Denk hierbij aan het BIMMEN, het gebruik van apps, digitale bouwtekeningen, urenregistraties, werkbonnen en cameratoezicht. Bouwmedewerkers moeten te allen tijde toegang hebben tot de meest actuele project- en productinformatie op hun laptop, smartphone of tablet. Digitale tekeningen, plannen en schema's moeten kunnen worden geraadpleegd en, indien nodig, aangepast.

## Een veilig en stabiel netwerk...

Mobiel internet maakt het uitvoeren van dergelijke digitale werkzaamheden heel wat eenvoudiger, maar dan wil je wel kunnen rekenen op een snelle, stabiele en vooral veilige verbinding. Voorwaarden die door het gebruik van een tijdelijke internetverbinding, nog vaak opgezet via een simkaart, niet altijd gegarandeerd zijn. Het beveiligen en stabiel houden van je netwerk wordt al snel ingewikkelder als iedereen in alle uithoeken van het bouwterrein met elk gewenst device verbonden wil zijn. In een tijd van alsmaar serieuzere cyberdreigingen is dit geen ideale startpositie.

## ... is dichterbij dan je denkt

Hoe mooi zou het zijn om mogelijke dreigingen al van het begin te kunnen stoppen? Met de cyberbeveiligingsoplossingen van CSN Groep in samenwerking met Fortinet wordt dit werkelijkheid. Zo ga je voor maximale veiligheid op de bouwplaats en een ononderbroken datastroom. Ontdek in deze whitepaper dat het niet lastig is om inzicht te krijgen in je systemen en in de status van je digitale veiligheid.

**“Een bouwplaats die stilligt, kost een bouwonderneming enorm veel geld. Om te voorkomen dat IT-problemen een bouw vertragen, sloegen we de handen in elkaar met Fortinet. Samen zetten we een ijzersterk netwerk op dat de veiligheid garandeert en de voortgang van de bouwwerken verzekert.”**

Robert van Kasteren, Sales Consultant CSN Groep





# Voordelen van een digitale bouwplaats...

Maar liefst 4 op 5 Nederlandse bouwondernemingen gebruiken momenteel een vorm van mobiele hardware en ervaren dagelijks de vele positieve aspecten van bouwsoftware. De juiste technologie maakt het verschil in de uitvoering van hedendaagse werkzaamheden. De voordelen zijn groot:

## 1 Onmiddellijke communicatie tussen alle belanghebbenden

De meeste bouwprojecten vereisen een constante communicatie tussen alle betrokken partijen. Elke onderbreking kan dan ook nadelig zijn voor de productiviteit binnen een project. Met mobiele technologie wordt non-stop communicatie een koud kunstje.

## 2 Toegang tot real-time informatie

Applicaties stellen buitendienstmedewerkers in staat documenten in te dienen op een gedeeld platform. Kantoormedewerkers kunnen deze vervolgens onmiddellijk bekijken. Op deze wijze zijn ze op de hoogte van het reilen en zeilen in het veld.

## 3 Hogere productiviteit

Met mobiele technologie kunnen medewerkers in het veld dagelijks rapporteren en onmiddellijk een antwoord ontvangen. Er is voor de medewerker geen reden meer om de bouwplaats te verlaten om informatie te verkrijgen. Een directe productiviteitswinst dus.

## 4 Betere organisatie

Met mobiele technologie hebben medewerkers alle nodige documenten binnen handbereik en zijn ze binnen enkele seconden eenvoudig te raadplegen.

## 5 Accurater administratie

Het maken van rapporten in het veld bespaart niet alleen een rit terug naar het kantoor, maar zorgt ook voor meer nauwkeurigheid.

## 6 Eenvoudige integratie

Mobiele applicaties vallen over het algemeen heel gemakkelijk te verenigen met je reeds bestaande systemen.



# ... en hoe ze te behouden

Eerder genoemde voordelen blijven enkel bestaan wanneer je investeert in hardware- en datasecurity. Ook jouw organisatie ontkomt er niet aan om het intellectueel eigendom te beschermen tegen cyberaanvallen als ransomware, phishing en datalekken. Naarmate het aantal potentiële doelen stijgt en de frequentie van bedreigingen hierdoor toeneemt, is het noodzakelijk om adequate securitymaatregelen te treffen om kwaadwillende buiten de deur te houden. Zeker wanneer je ook netwerktoegang verleent aan mensen buiten je organisatie.

NextGen securitymaatregelen helpen je bouwbedrijf bekende en onbekende bedreigingen op meerdere lagen in je omgeving te detecteren. Daarnaast kan een interne netwerksegmentatiestrategie helpen bij het detecteren en automatisch indammen van alle soorten bedreigingen. Zo hoef je bij een aanval slechts een deel van je netwerk 'op te sluiten' en blijven andere delen ongeschonden.

## De verdediging is de beste aanval

Wat doe je als je netwerk is gehackt? Dit is een vraag die elke organisatie zich moet stellen. Want als het dan toch een keer gebeurt, dan wil je dat de impact minimaal is. Zorg er daarom voor dat de verdediging klaarstaat en segmenteer je netwerk. Dit houdt naast een opgedeeld netwerk ook in dat er beveiligingszones binnen je netwerk zijn gedefinieerd. Op basis van vooraf ingestelde parameters en firewalls wordt er binnen je beveiligingsbeleid afgesproken wie met welk apparaat toegang krijgt tot deze zones.

Fortinet stelt je via segmentatiestrategieën in staat een aanval proactief te isoleren, waardoor de mogelijkheid tot verspreiding van bijvoorbeeld ransomware wordt beperkt. Zonder de juiste segmentatie kunnen cyberdreigingen zich nu eenmaal makkelijk door je netwerk verspreiden. Ook naar je back-ups, waardoor herstel veel moeilijker uit te voeren is en bouwvertraging akelig dichtbij kan komen.

## Na actie volgt reactie

Alleen een firewall gebruiken om jouw in- en uitgaande internetverkeer te reguleren is vandaag de dag niet meer voldoende. Daarom biedt CSN Groep jouw organisatie de juiste bescherming door middel van een adequate netwerkinrichting. Door het plaatsen van 'sensoren' binnen de FortiGate firewalls worden patronen binnen het netwerkverkeer gedetecteerd. De sensoren kunnen, klant specifiek, op tal van strategische plaatsen worden ingezet en signaleren en blokkeren verdachte activiteiten. Door het gebruik van CSN Managed Detection and Response (MDR) zal de malware in vrijwel alle gevallen niet meer bij de server komen en wordt de aanval afgewend.

Dankzij onze kennis ontzorgen we jouw organisatie door de sensoren actief aan te passen op basis van actuele cyberdreigingen. Zodra de omgeving naar wens is afgestemd, wordt je omgeving gemonitord op zogenoemde 'Indicators of Compromise' waarna de sensoren 24/7 ingrijpen bij het detecteren van bedreigingen.

## Met MDR tackle je de volgende uitdagingen:

- **Bescherm je endpoints tegen malware**  
MDR biedt je organisatie een endpoint beschermingsplatform dat specifiek 'endpoints' als laptops en smartphones beschermt tegen malware-aanvallen.
- **Roep de 'laterale verplaatsing' van bedreigingen een halt toe**  
Een van de meest voorkomende manieren waarop hackers een netwerk in gevaar brengen is via een zogenaamde 'laterale verplaatsing'. Heeft een hacker eenmaal toegang tot een netwerk, dan probeert de aanvaller dieper door te dringen om gevoelige gegevens en privileges te verkrijgen. Om toegang tot het netwerk te houden, blijft hij zich door het netwerk bewegen. MDR-services detecteren deze laterale bewegingen en stellen jouw team in staat om op tijd actie te ondernemen.
- **Detecteer interne beveiligingsinbreuken**  
Een foute klik is snel gemaakt. Medewerkers kunnen bewust en onbewust interne beveiligingsregels overtreden. Wanneer deze situatie zich voordoet kan MDR je helpen onderzoeken wat er precies is gebeurd en waarom.



# Ook je digitale bouwplaats optimaal beschermen?

Stabiele en veilige verbindingen voor bedrijfsdata en applicaties zijn essentieel voor iedere organisatie. Gebruikers en data zijn tegenwoordig overal en dat maakt het realiseren én beheren van een bedrijfsnetwerk steeds complexer. Door gebruik te maken van de juiste tooling wordt het netwerk inzichtelijk en zijn risico's snel te detecteren.

**Ga voor maximale veiligheid op de bouwplaats!  
Speel op zeker met CSN Groep en Fortinet.**

Onze experts geven je graag gericht advies bij de keuze, implementatie en het beheer. Aarzel niet om contact met ons op te nemen en ga vol voor de toekomst van je bouwonderneming.

## CONTACT

Fokkerstraat 12

3833 LD Leusden - Nederland

+31 88 999 0999

[info@csngroep.nl](mailto:info@csngroep.nl)

