NU BOUWEN AAN MORGEN
verkenning bouw & infra 2030

Democratie besluitvorming

Technologie Digitalisering | Financieel | Mens / Sociaal | Duurzaamheid Circulariteit

Digitale veiligheid: wie kun je in 2030 nog vertrouwen?

Bron: Rawpixel

Bouwend Nederland
de vereniging van bouw- en infrabedrijven

Digitale veiligheid: wie kun je in 2030 nog vertrouwen?

Samenvatting; Veiligheid in de bouw is al lang een belangrijk thema. En dan gaat het vooral om veiligheid op de bouwplaats. Maar ook digitale veiligheid zal een steeds grotere rol gaan spelen. Door het gebruik van systemen als BIM is steeds meer informatie online. Deze systemen zijn daarmee een toenemend doelwit voor hackers. Door de situatie omtrent het coronavirus vinden ook veel werkzaamheden op afstand en vanuit huis plaats. Hoe zeker ben je er dan als bouw- of infrabedrijf van dat deze data ook niet voor kwaadwillenden toegankelijk is?

Verder zijn er specifieke kenmerken in de bouw en infra die het aannemelijk maken dat de bouwsector kwetsbaar zal zijn voor belangrijke digitale bedreigingen. Bovendien is het waarschijnlijk dat de publieke sector door ontwikkelingen als 'deepfakes' en AI op een andere manier naar digitale veiligheid zal kijken, maatregelen zal nemen en wetgeving gaat maken. Tenslotte is het goed denkbaar dat grote bouwprojecten tegen 2030 te maken krijgen met georganiseerde weerstand van bewoners die zich verenigen via digitale kanalen zoals sociale media, en door fake nieuws.

Relevantie
In 2030 zal digitale veiligheid dus een belangrijk onderwerp zijn. Weten met wie je zaken kunt doen en je bedrijf, mensen en klanten goed beveiligen zullen de aandacht vragen. De bouw- en infrasector, waar het vaak gaat om projecten van miljoenen of zelfs miljarden, kan zeker een potentieel doelwit zijn voor hackers. Doordat vanwege Covid-19 veel meer mensen thuiswerken, is op afstand werken nu heel normaal, maar daarmee is ook het risico van kwetsbaarheden zeker toegenomen. Dat risico zal in 2030 niet verminderd zijn. Het is daarom zaak dat de sector zich daar nu al op voorbereid, zich klaarmaakt om digitaal "smart" te worden en digitale veiligheid vooropstelt.

Achtergrond
Het Global Risk Report 2019 van het World Economic Forum stelt dat "Cyber-attacks" en "Data Fraud or theft" in de top 5 van belangrijkste bedreigingen staan.

Natuurlijk: in sectoren zoals de financiële sector speelt fraude een nog grotere rol. Maar ook in de bouw en infra gaat veel geld om. Bovendien zijn de projecten vaak complex waardoor fraude moeilijker te detecteren is. Uit Amerikaans onderzoek blijkt dat de vastgoed- en de bouwsector de grootste verliezen kennen als het gaat over fraude (bron: GRFCPA).

Meer internet en online-oplossingen zoals BIM en platforms van projectmanagement maken bouw- en infrabedrijven kwetsbaarder voor hackers en cyberaanvallen. Met de toename van thuiswerken door kantoormedewerkers wordt ook veel informatie gedeeld. Er wordt vergaderd via applicaties zoals Zoom en sinds de start van de Covid-19-crisis zijn er al meer dan 1700 nieuwe domeinnamen met Zoom in de naam geregistreerd, vaak wordt dit door criminelen gedaan die hiermee willen proberen om links te generen voor phishing (bron OECD). Daarnaast worden digitale toepassingen ook steeds meer gebruikt in bouwprojecten voor slimme huizen, kantoren en infrastructuur. Uit onderzoek van Gemalto in 2019 blijkt dat maar een beperkt aantal bedrijven in staat is om IoT datalekken op te sporen. Het is daarom belangrijk dat bouwbedrijven nadenken over digitale veiligheid.

Uitdaging
Specifiek voor de bouw en infra is er een aantal factoren die de sector extra kwetsbaar maken voor digitale risico's.

In de eerste plaats wordt er op veel locaties gewerkt en worden medewerkers geacht mobiel bereikbaar te zijn op deze locaties. Ze moeten vanaf diverse locaties kunnen inloggen op bedrijfsomgevingen en maken vaak gebruik van eigen hardware waarmee de kwetsbaarheid toeneemt. Door Covid-19 is het aantal handelingen dat op afstand plaatsvindt door medewerkers die vanuit huis toegang hebben tot BIM-systemen alleen maar toegenomen. Uiteraard wil je als bedrijf je medewerkers de mogelijkheden bieden om vanuit huis te kunnen werken, maar het is belangrijk om daarbij de beveiliging goed op orde te hebben en deze ook regelmatig te testen om hiermee potentiële kwetsbaarheden vroegtijdig te ontdekken.

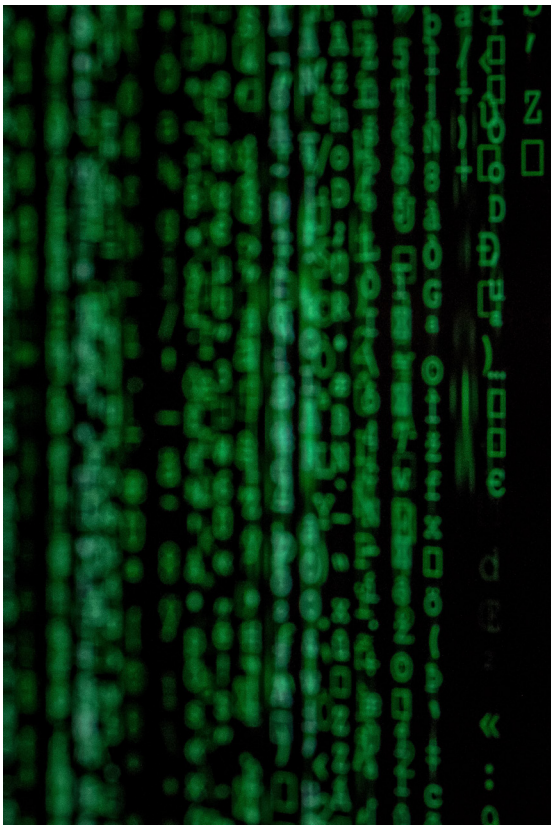
In de tweede plaats werken vaak verschillende partijen samen in de bouw en infra. Hierdoor worden veel gevoelige data en informatie, zoals persoonsgegevens en financiële details, uitgewisseld tussen bedrijven.

Tenslotte is er veel tijdelijk personeel en veel verloop in de bouw en infra waardoor het lastig is om digitale veiligheid echt goed in de werkmethodes en procedures te krijgen.

Uit onderzoek van HUB International blijkt dat de bouwsector achterloopt in investeringen in digitale veiligheid en daarmee extra kwetsbaar is voor digitale risico's en hackers.

Actie
De bouwsector moet digitale veiligheid als belangrijk item oppakken. Het CIOB heeft hiervoor 6 principes opgesteld:

1. Pas een security-minded aanpak toe op je professionele en persoonlijk leven;
2. Neem een leiderschapsrol en pas verantwoordelijk beoordelings-vermogen toe;
3. Zorg dat je op de hoogte bent van wet- en regelgeving, begrijp de intentie en zoek naar verdere verbeteringen;
4. Zorg voor echt beveiligde communicatie;
5. Implementeer blijvende systemen voor 'security governance';
6. Draag bij aan publieke en professionele veiligheid.



Het CIOB heeft een handige checklist opgesteld om te komen tot een goed digitaal veiligheidsplan. Daarnaast is het zaak de juiste maatregelen te treffen voor hard- en software, om de juiste updates te installeren en te zorgen voor een back-up waarop je kunt terugvallen als er toch iets misgaat.

Resultaat
Hoe kwetsbaar de digitale infrastructuur is, werd in 2017 duidelijk toen in Duitsland een groep hackers NetCom BW infiltreerde. Dit bedrijf was echter niet het primaire doel van de hackers, maar het moederbedrijf: een groot energiebedrijf en onderdeel van de door de overheid aangemerkte kritische infrastructuur.

Hoe meer betrokken partijen, hoe kwetsbaarder de fysieke infrastructuur dus. Uit het Duitse voorbeeld blijkt dat dit zeker het geval is voor onze energie- en telecominfrastructuur. In 2030 zal die kwetsbaarheid zeker zijn toegenomen door de opkomst van slimme steden en zelfrijdende voertuigen.

Gelukkig zijn er ook startups als het Deense Dartrace dat een soort immuunsysteem voor digitale veiligheid heeft ontwikkeld. Of zoals het Nederlandse Deeptrace Labs dat een soort antivirus construeerde om digitale identiteit beter te kunnen controleren en te onderscheiden van kwaadwillenden.

Impact

De investering in digitale veiligheid wordt steeds belangrijker voor de bouw- en infrasector. Digitalisering is niet alleen een hulpmiddel bij de uitvoering van bouwprojecten, maar wordt meer en meer onderdeel van het primaire proces. Slimme meters voor energievoorziening, sensoren in huizen en gebouwen en slimme infrastructuur in wegen en tunnels maken digitale veiligheid tot een belangrijk aandachtspunt bij het ontwerp van gebouwen en infrastructuur.

En nu?

De bouwsector investeert van oudsher minder in IT en vaak nog minder in IT-security. In 2030 zal dit echt niet meer kunnen en moet een bouw- of infrabedrijf dus de kennis in huis hebben, zorgen dat het onderdeel is van het primaire proces en de juiste maatregelen moeten hebben genomen om eventuele problemen aan te kunnen.

Acties die je als bouw- of infrabedrijf vandaag al kunt ondernemen zijn:

- **Check of je digitale veiligheids-maatregelen voldoende zijn. Zo niet, maak dan een plan om deze up-to-date te maken.**
- **Stel vast wie in je bedrijf verantwoordelijk is voor de digitale veiligheid. Is er een calamiteiten-procedure en wordt deze ook actief gemonitord en getest?**
- **Hoe heb je als bedrijf digitale veiligheid meegenomen in je projecten? Heb je hiervoor budget gereserveerd en heb je alle aspecten hierin meegenomen?**

Links

- Dealing with digital security risk during the Coronavirus (COVID-19) crisis
- The Global Risks Report 2019 14th Edition
- Cybersecurity In Construction: What You Need to Know
- Implications of IoT Security in Construction Use Cases
- Perspective Why Cyber Should be Higher on Contractors' Risk Agendas Cyber security remains low on construction
- The role of security in the construction industry
- Cyber Risk Update for Construction Companies | Stoel Rives - Global Privacy & Security Blog
- Data Breaches, Cyber Security and the Construction Industry
- Internet Companies Prepare to Fight the 'Deepfake' Future
- The Future is Fake - The Startup
- https://www.uscybersecurity.net/deepfake/
- Even the AI Behind Deepfakes Can't Save Us From Being Duped
- Deepfake Legislation: A Nationwide Survey
- DeepFake and the Future of Reality
- Which Industries are Hardest Hit by Fraud? | GRF CPAs & Advisors
- https://www.investopedia.com/articles/investing/072115/why-these-industries-are-prone-corruption.asp
- Pulling fraud out of the shadows
- Cybercrime in Construction Industry
- Zes dingen die je moet weten over iot-security
- Germany's Cybersecurity Teams Fight 'Ticking Time Bombs'
- Launch of the Cybersecurity Label cyber-safe.ch in December 2019
- Cybersecurity startup Darktrace reached $1.65 billion valuation in just 5 years
- 2016 Construction Technology Report Stats [Infographic]
- Data Breaches, Cyber Security and the Construction Industry

Bibliografie

- The Global Risks Report 2019 14th Edition, World Economic Forum