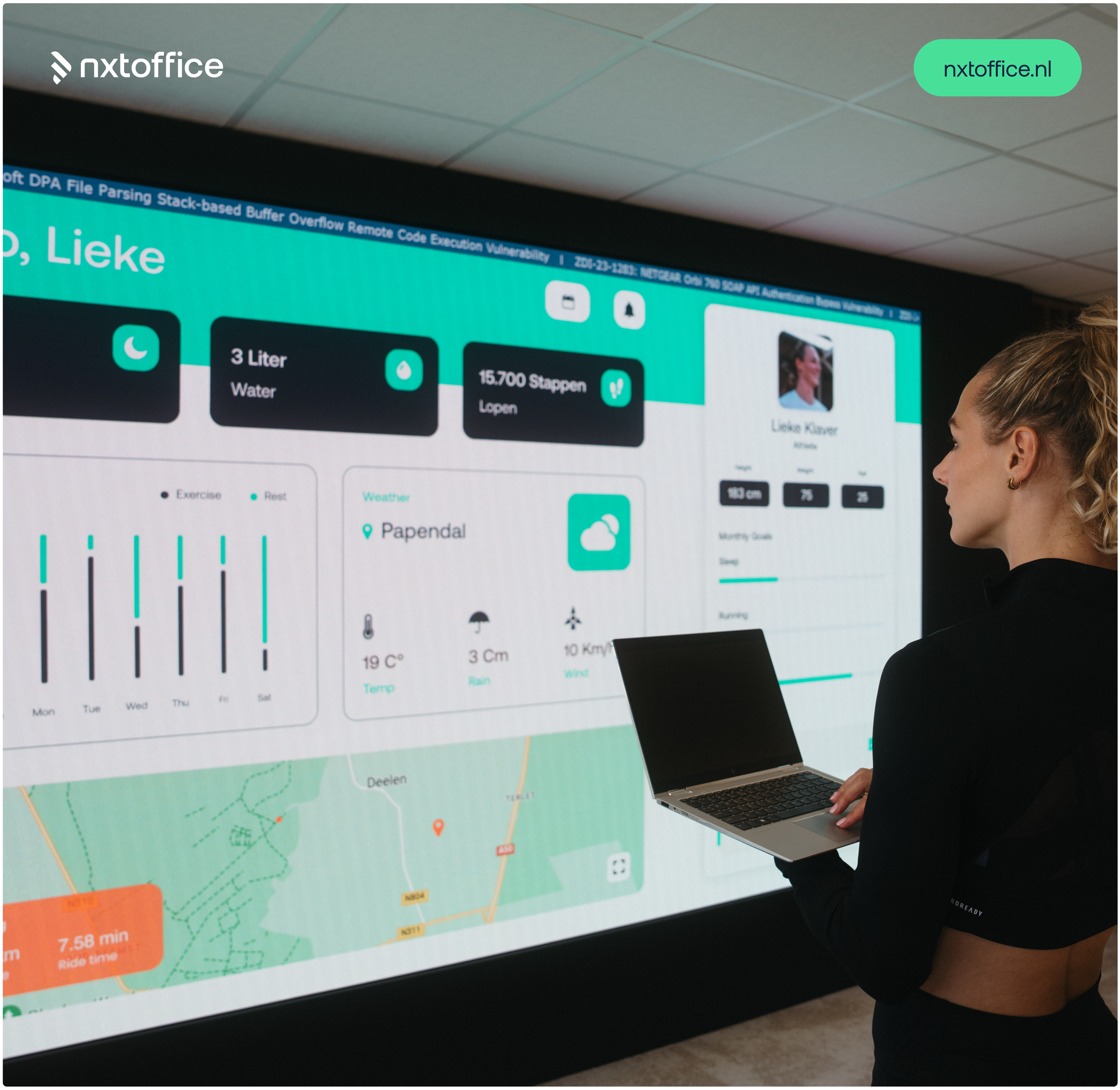
nxtoffice

nxtoffice.nl



Doe de check

Voorkom downtime en kies voor een bedrijfsnetwerk dat écht werkt

Het beveiligen van je bedrijfsnetwerk. Waar begin je?

In een wereld waarin bedrijfsvoering steeds digitaler wordt, is een goed beveiligd bedrijfsnetwerk geen luxe, maar een absolute noodzaak. Cyberaanvallen kosten tijd en geld. Hackers richten zich steeds vaker op het MKB. Eén zwakke schakel kan je bedrijf stilleggen, met gemiddeld € 8.000 verlies per uur als gevolg. Met nxtoffice bouw je aan een veilig en toekomstbestendig netwerk, zodat je cyberdreigingen vóór blijft.

De 5 meest voorkomende dreigingen voor je bedrijfsnetwerk

1. Malware-infecties

Kwaadaardige software verspreidt zich razendsnel via onbeveiligde netwerken en apparaten. Voorbeelden zijn:

> Ransomware – gijzelt je bestanden.

> Spyware – volgt je online gedrag en verzamelt gegevens.

> Wormen en trojans – dringen binnen via beveiligingslekken.

2. Phishing & social engineering

Medewerkers ontvangen ogenschijnlijk legitieme e-mails met de vraag om op links te klikken of inloggegevens achter te laten. Vaak is dit het begin van een groter datalek of netwerkovername.

3. DDoS-aanvallen

Je bedrijfsnetwerk of website wordt overspoeld met verkeer, waardoor systemen onbereikbaar worden. Dit treft vooral bedrijven met online dienstverlening.

4. Man-in-the-middle aanvallen

Een hacker onderschept communicatie tussen twee partijen en wijzigt bijvoorbeeld bankgegevens op facturen.

5. De grootste dreiging: het menselijke gedrag

Je kunt je techniek nog zo goed op orde hebben — firewalls, antivirussoftware, encryptie — maar het gedrag van medewerkers is vaak de grootste risicofactor:

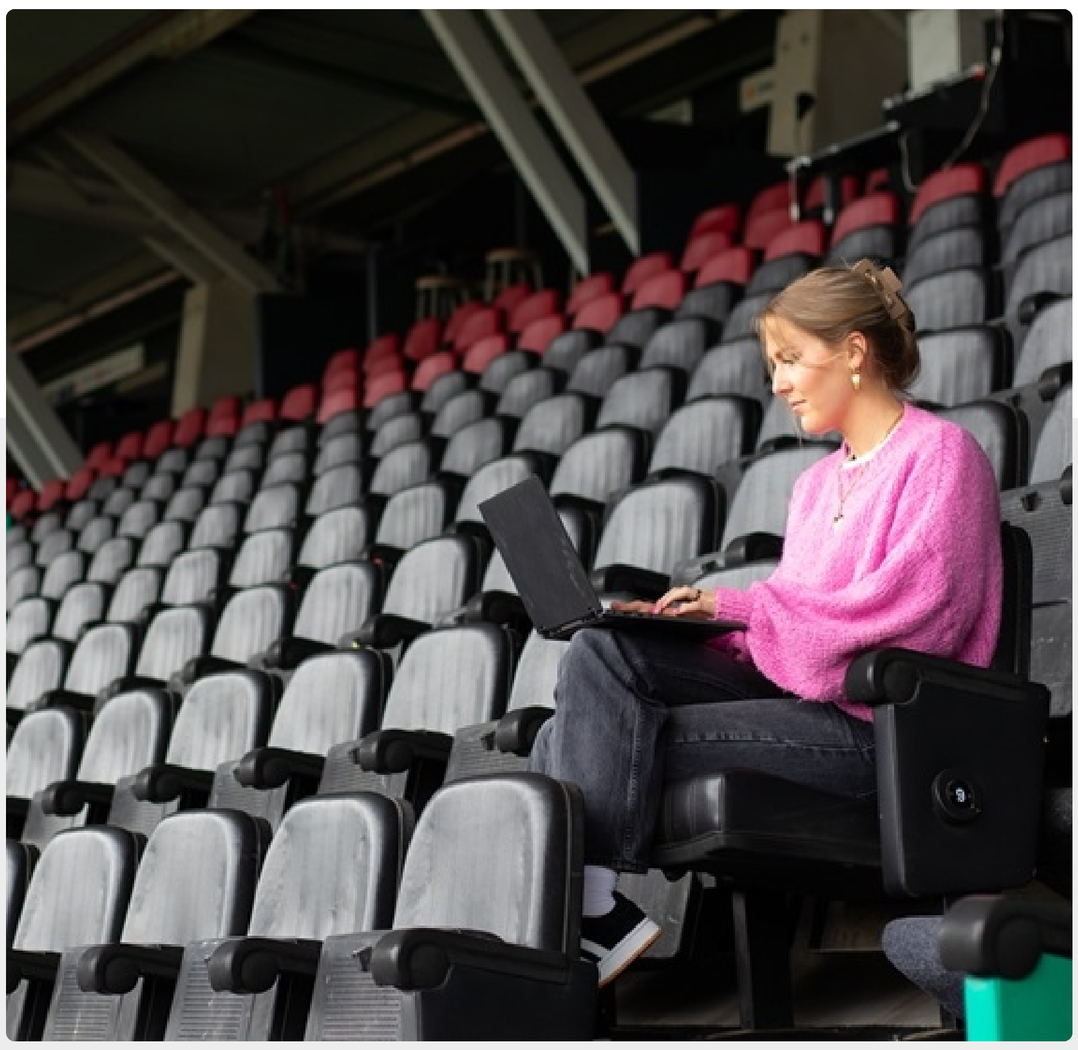
> Verbinden met openbare wifi zonder VPN.

> Klikken op verdachte links of bijlagen.

> Gebruik van zwakke wachtwoorden of hergebruik ervan.

De gevolgen van een slechte netwerk-beveiliging?

- Stilstand van bedrijfsprocessen
- Financiële schade door afpersing of boetes
- Datalekken met reputatieschade
- Verlies van klantvertrouwen
- Toegang tot je netwerk door derden zonder dat je het weet



nxtoffice

nxtoffice.nl

Spoor kwetsbaarheden vroegtijdig op met de netwerk-security scan

Om als organisatie en ook als werkgever toekomstbestendig te zijn is het van cruciaal belang om mogelijke kwetsbaarheden in het bedrijfsnetwerk vroegtijdig op te sporen. Heeft jouw bedrijf al een duidelijke strategie wat betreft onderstaande punten?

> Up-to-date software en apparaten
> Sterk wachtwoordbeleid
> Firewall & netwerksegmentatie
> VPN voor extern werken
> Gedragsbewustzijn trainen
> Beveilig IoT-apparatuur
> Incident response plan

43% van de cyberaanvallen treft het MKB. Ben jij goed voorbereid?

Vraag vandaag nog geheel vrijblijvend onze netwerk-security check aan en krijg een concreet inzicht in hoe goed jouw bedrijf beveiligd is tegen de geavanceerde cyberdreigingen anno nu.

Neem contact op met Michiel of bezoek de website

+31 88 566 7103

m.huising@nxtoffice.nl

nxtoffice.nl