

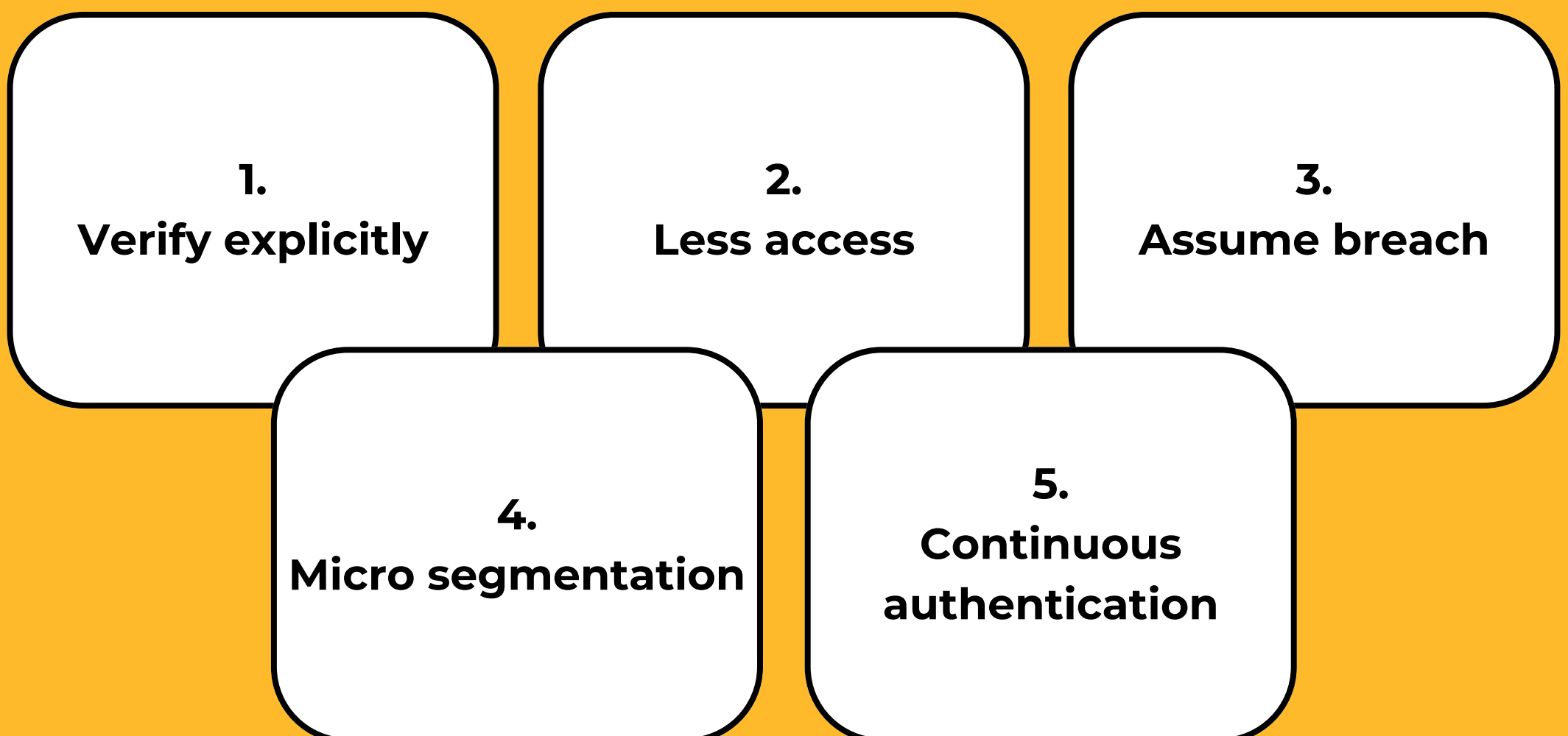
introduktion til  
**Zero Trust arkitektur**

*"Never trust, always verify"*





# Indenfor Zero Trust fokuseres der på 3-5 overordnede principper



Ved at overholde disse principper kan organisationer skabe et mere sikkert og modstandsdygtigt miljø for deres kritiske aktiver og data.





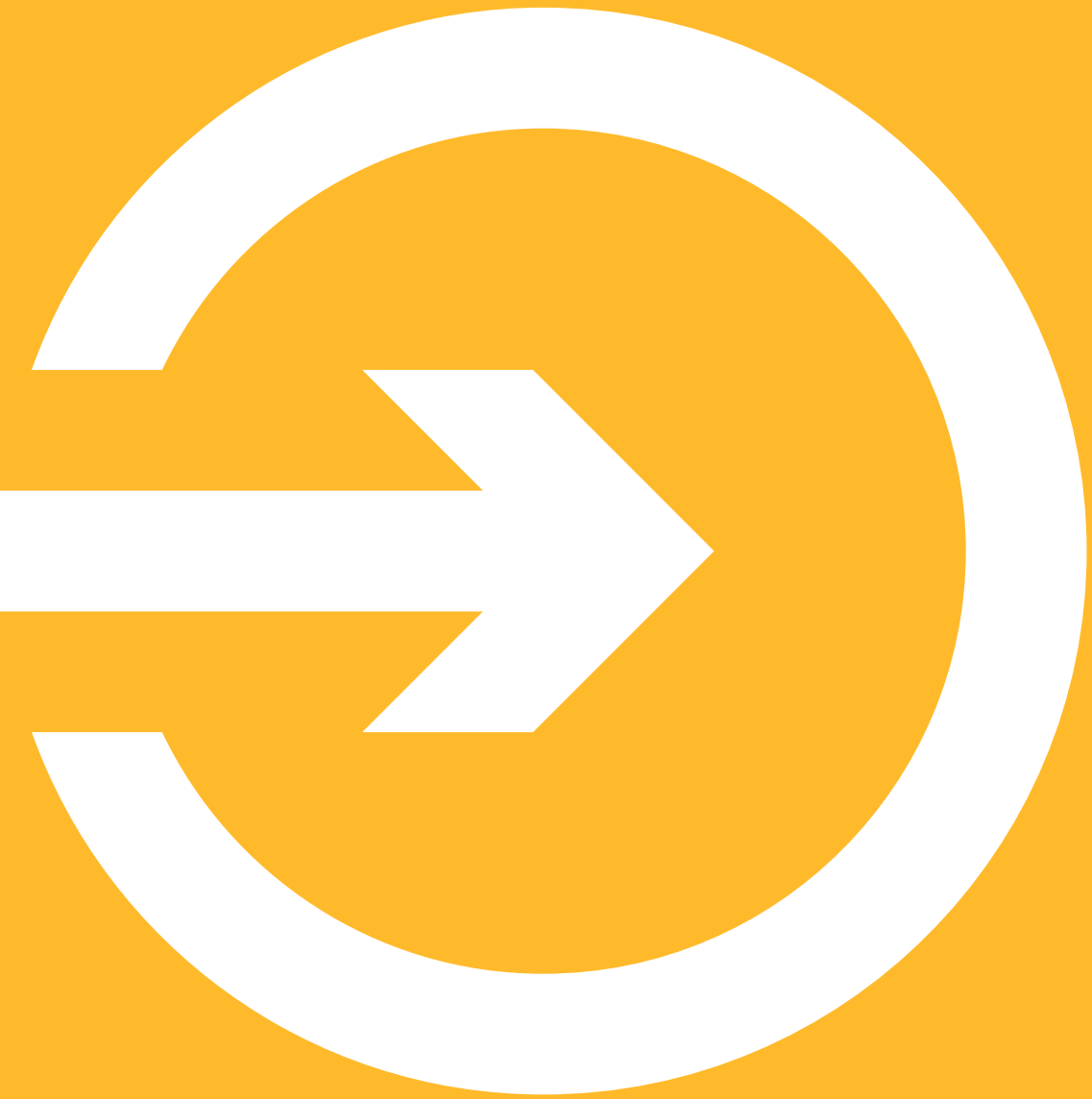
**1.**

## **Verify explicitly**

**Stol på ingen som standard.**

**Bekræft altid identiteten og godkendelsen af enhver bruger og enhed, der forsøger at få adgang til ressourcer, uanset deres placering eller netværkskontekst.**





2.

## Less access

**Giv brugere og systemer det minimumsniveau af adgang, der kræves for at udføre deres opgaver.**

**Undgå at give for brede tilladelser.**



**3.**

## **Assume breach**

**Gå ud fra den antagelse, at et brud på sikkerheden altid er mulig.**

**Design sikkerhedsforanstaltninger for at afgrænse og begrænse potentiel skade i tilfælde af et brud.**





4.

## Micro segmentation

**Opdel netværket i små, isolerede segmenter, hver med sine egne adgangskontroller.**

**Dette begrænser lateral bevægelse for potentielle angribere.**





**5.**

## **Continuous authentication**

**Autentificer brugere og enheder  
løbende, ikke kun ved login.**

**Dette sikrer, at tillid aldrig er  
antaget, og at adgangen  
overvåges løbende.**



# OMNIUM \_IMPROVEMENT



**Marie Emilie Gerrild Petersen**

Senior consultant  
mp@omnium.dk



**Jack Kaare Ekman**

Partner  
jke@omnium.dk