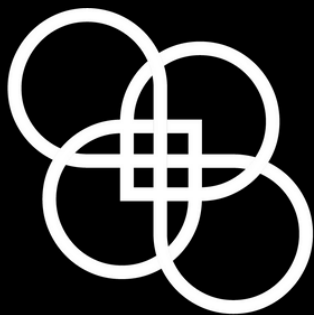




***IS JE BACK-UP
VEILIG?
CONTROLEER HET !***



CHECKLIST



IS JE BACK-UP VEILIG? CONTROLEER HET!

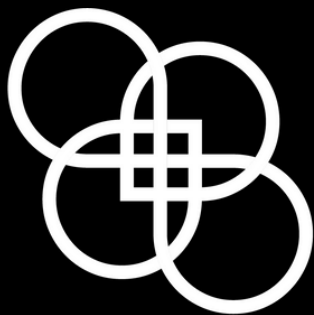
CHECKLIST

IMMUTABLE BACK-UP

- ☐ Is je back-up niet te wissen of aan te passen?
- ☐ Heb je deze beschermd tegen ransomware en menselijke fouten?
- ☐ Is er sprake van end-to-end encryptie? (tijdens opslag én transport?)
- ☐ Heb je de toegang tot back-ups strikt geregeld middels het Zero Trust beleid?

SNEL EN SLIM HERSTEL

- ☐ Kun je binnen je Recovery Time Objective (RTO) weer operationeel zijn?
- ☐ Zijn je back-ups afgestemd op je Recovery Point Objective (RPO)?
- ☐ Is er sprake van versiebeheer?
- ☐ Heb je de back-up getest met een realistische herstel oefening?



IS JE BACK-UP VEILIG? CONTROLEER HET!

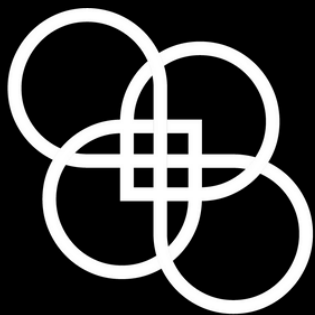
CHECKLIST

LOCATIE, LOCATIE, LOCATIE

- ☐ Worden je back-ups offsite of in de cloud opgeslagen?
- ☐ Hanteer je de 3-2-1-regel?
 - 3 kopieën
 - 2 soorten media
 - 1 offsite back-up
- ☐ Zijn je datacenters aantoonbaar veilig (bijv. ISO 27001)

MONITORING & ALARMBELLEN

- ☐ Wordt elke back-up automatisch gecontroleerd op fouten of uitval?
- ☐ Ontvang je meldingen bij mislukte back-ups of verdachte activiteiten?
- ☐ Wordt toegang tot de back-up omgeving gelogd en bewaakt?



IS JE BACK-UP VEILIG? CONTROLEER HET!

CHECKLIST

BELEID & COMPLIANCE

- ☐ Bestaat er een actueel, gedocumenteerd back-upbeleid?
- ☐ Is je back-upstrategie compliant met de AVG en (komende) NIS2-wetgeving?
- ☐ Is er één verantwoordelijke binnen de organisatie die toezicht houdt?

Wees niet de volgende die zegt:
“We dachten dat alles geregeld was..”

Neem geen genoegen met we maken
gewoon een standaard back-up.
Dat is hetzelfde als denken dat je
parachute werkt, zonder vooraf te
checken of hij open gaat.

