

WHITEPAPER: Een sterke cybersecuritycultuur: van verplichting naar versterking

Subtitel: Hoe je als organisatie structureel veiliger wordt door gedragsverandering – en hoe Secwiz je daarbij helpt.

1. Inleiding

De menselijke factor is verantwoordelijk voor meer dan 90% van alle datalekken en cyberincidenten. Tegelijkertijd is het gedrag van medewerkers ook de grootste kans op structurele verbetering. Maar hoe ontwikkel je als organisatie een cultuur waarin veilig gedrag vanzelfsprekend wordt?

2. Wat is een positieve cybersecuritycultuur?

Het NCSC stelt: “Een positieve cybersecuritycultuur is een werkomgeving waarin medewerkers zich bewust zijn van hun eigen rol in informatiebeveiliging, waarin veilig gedrag wordt gestimuleerd, gewaardeerd en gefaciliteerd.”

Dat betekent onder andere:

- Veilig gedrag belonen in plaats van straffen
- Voorbeeldgedrag door management
- Open communicatie over fouten en incidenten
- Regelmatige training en bewustwording

3. MKB: kwetsbaar en onder druk

Voor MKB-organisaties is het vaak lastig om cybersecurity structureel aan te pakken:

- Te weinig tijd of kennis in huis
- IT-partners focussen op techniek, niet op gedrag
- HR mist vaak tooling of handvatten
- Groeiende druk door NIS2, AVG en verzekeraars

4. Phished via Secwiz: gedragsverandering als dienst

Secwiz is partner van Phished.io: een bewezen platform voor security awareness & gedragsverandering.

Wat maakt Phished anders?

- **Realistische phishing simulaties** op basis van AI
- **Persoonlijke trainingspaden** voor iedere medewerker
- **Microlearning** die aansluit op actuele dreigingen
- **Volledig geautomatiseerd**: geen extra werk voor IT of HR
- **Relevante dashboards** en rapportages voor compliance en audits
- **Ingebouwde ondersteuning voor NIS2 en AVG**

Maar we doen meer dan het leveren van tooling. Vanuit Secwiz brengen we ook **expertise en begeleiding** om security structureel op een hoger niveau te tillen. We helpen bij het intern verankeren van security awareness, geven advies op maat en ondersteunen waar nodig bij beleid, communicatie en naleving.

5. Ervaringen uit de praktijk

Gebruikers waarderen vooral:

- de korte, heldere leermomenten
- het realistische karakter van de simulaties
- de directe impact op gedrag
- de eenvoudige implementatie en minimale belasting
- het feit dat het inspeelt op zowel werk- als privécontext

6. De volgende stap: concreet aan de slag

Benieuwd hoe jouw organisatie op een laagdrempelige manier aan een positieve cybersecuritycultuur kan bouwen?

Wij bieden:

- vrijblijvende demo of proefperiode
- begeleiding bij implementatie
- communicatiekits voor intern gebruik
- support bij audits en compliance
- strategisch advies van onze specialisten

Neem contact op met Secwiz – en maak van je medewerkers de sterkste schakel.