ADVIESKAART

Effectieve communicatie

Q2 2026

Cyber Weerbaarheidscentrum
BRAINPORT
Voor hightech- & maakindustrie in NL

Digitale veiligheid valt of staat bij de mens. Onduidelijke instructies of technisch jargon zorgen voor een kloof tussen beleid en de werkvloer. Effectieve communicatie is daarom broodnodig.

1 > VERTAAL TECHNIEK NAAR DE DAGELIJKSE PRAKTIJK

Voorkom dat medewerkers afhaken door technisch jargon. Gebruik liever alledaagse vergelijkingen om abstracte begrippen tastbaar te maken. Dit resulteert in een gemeenschappelijke taal die de drempel voor vragen verlaagt.

Voorbeeld: Leg Multi-Factor Authenticatie (MFA) uit als een tweede slot op de deur. Zelfs als iemand je sleutel steelt, komen ze nog niet binnen.

2 > COMMUNICEER HET 'WAAROM', NIET ALLEEN HET 'WAT'

Regels zonder context worden ervaren als een last. Als medewerkers begrijpen welk risico een maatregel afdekt, groeit de intrinsieke motivatie om deze na te leven.

Voorbeeld: Koppel een verbod op onbekende USB-sticks aan het risico op malware, vergelijkbaar met het weren van ongecontroleerde onderdelen in een productielijn.

3 > GEBRUIK HERHALING EN VASTE MOMENTEN

Security vraagt blijvend om aandacht. Korte, regelmatige updates werken beter dan jaarlijkse complexe trainingen. Gebruik middelen als intranet, posters of werkoverleggen. Maak het onderdeel van het normale werkproces, net als veiligheidsinstructies op de werkvloer.

4 > STIMULEER MELDEN ZONDER SCHULD

Een bedrijf dat vragen en meldingen aanmoedigt, is structureel veiliger, want meldingen beperken schade. Als medewerkers fouten kunnen melden zonder angst voor straf draagt dat bij aan de collectieve veiligheid.

5 > PAS COMMUNICATIE AAN PER DOELGROEP

Niet elke afdeling kampt met dezelfde risico's. Zorg dat de boodschap voor een productiemedewerker anders is dan voor een kantoorfunctie. Sluit aan bij hun specifieke dagelijkse realiteit om de relevantie te vergroten.

6 > MEET, EVALUEER EN VERBETER CONTINUE

Effectieve communicatie vraagt om constante kwaliteitscontrole. Actief kijken naar de aard van meldingen, gestelde vragen en het type incidenten, geeft inzicht in wat wel en niet overkomt bij de medewerkers. Gebruik feedback uit de organisatie om boodschappen aan te scherpen en aan te passen aan het veranderende dreigingslandschap.

i

Meer informatie over dit onderwerp deelt Cyber Weerbaarheidscentrum Brainport met haar participanten. Ook lid worden van deze stichting zonder winstoogmerk? Bezoek www.cwbrainport.nl of mail naar info@cwbrainport.nl.

Met dank aan

BRAINPORT EINDHOVEN
METROPOOL REGIO EINDHOVEN
Provincie Noord-Brabant