



Digitale weerbaarheid van een organisatie vraagt om een bedrijfscultuur die verbetering aanmoedigt en mogelijk maakt. Personeel moet zich veilig voelen en merken dat veilig gedrag gewaardeerd wordt.

1 > ZORG VOOR DUIDELIJKE EN TOEGANKELIJKE CYBERSECURITYREGELS

Zorg dat regels bruikbaar zijn en toegankelijk voor iedereen. Beoordeel en test regelmatig of ze hun doel dienen; ze moeten aansluiten bij de behoefte van personeel om werk gedaan te krijgen. Vraag actief om feedback. Communiceer veranderingen in de hele organisatie en archiveer oude regels om verwarring te voorkomen. Leg elke nieuwe werknemer de regels uit tijdens de onboarding.

2 > LEIDING GEEFT HET GOEDE VOORBEELD

Leidinggevendenden nemen hun verantwoordelijkheid. Ze tonen zelf cyberveilig gedrag en communiceren het belang naar de medewerkers. Ze stimuleren veilig gedrag en nemen prikkels weg die leiden tot slecht beveiligingsgedrag.

3 > STIMULEER OVERNAME VAN BESTAAND CYBERVEILIG GEDRAG

Medewerkers kopiëren – vaak onbewust - gangbaar gedrag in hun omgeving. Identificeer wenselijk en onwenselijk gedrag in je organisatie en de drijfveren erachter. Maak een plan om positieve normen te versterken en belemmerende gewoontes aan te pakken. Voer uit, evalueer en stel bij waar nodig.

4 > OMARM IDEEËN, VRAGEN, ZORGEN EN FOUTEN

Het moet mogelijk zijn om snel vragen te stellen of beveiligingsproblemen te melden. Betrokkenen bij een incident krijgen geen straf voor een vergissing. Onderzoek naar een incident is bedoeld om te leren en te verbeteren, niet om te wijzen.

5 > VERANDERING IS EEN KANS VOOR VERBETERING

De kern van een cyberweerbare organisatie is het vermogen om aan te passen aan nieuwe technologieën en het alsmaar veranderend dreigingslandschap. Zorg dat mensen risico's en mogelijkheden goed afwegen en bewuste keuzes maken. Blijf evalueren en bijstellen.

6 > ER IS BEGRIP VOOR HET BELANG VAN CYBERSECURITY

Medewerkers begrijpen dat cybersecurity bedoeld is om belangrijke systemen goed te laten werken en gevoelige informatie te beschermen. Ze zijn zich bewust van hun eigen gedrag en zien securitybeleid niet als obstakel voor hun werk. De organisatie probeert negatieve effecten van beveiligingsmaatregelen op de werkvloer te minimaliseren.

Meer informatie met suggesties om toe te passen, staan op de website van het [Nationaal Cyber Security Centrum](#). De informatie is gebaseerd op het [Engelstalige origineel](#)



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