10 VUISTREGELS VOOR CYBER-SECURITY

Een handreiking voor bestuurders en ondernemers

Voor de digitale economie

NEDERLAND ICT

Noodzakelijke maatregelen voor cybersecurity beginnen bij bewustzijn. Bewustzijn voor cybersecurity is nodig in de hele organisatie. Actie kan pas volgen op die bewustzijn als ook de top van een organisatie bewust is van de noodzaak.

Met deze 10 vuistregels voor bestuurders en ondernemers geeft Nederland ICT een handvat om cybersecurity op de agenda van de directie te zetten.

1. Ik weet op welke manier ICT en internet bijdragen aan de (vitale) bedrijfs- en productieprocessen van de organisatie en welke gegevens de organisatie beheert.
2. Ik weet welke risico's de organisatie loopt in geval van verstoring of cyberaanval, ook wanneer deze verstoring elders in de keten plaatsvindt.
3. Ik weet aan welke eisen en regels de organisatie moet voldoen met betrekking tot gegevensbescherming, ik ben op de hoogte van de inwerkingtreding van de GDPR in mei 2018.
4. Ik weet wie in de organisatie verantwoordelijk is voor beveiliging: deze functionaris is voorbereid en heeft mandaat en voldoende middelen (bijv. 10% van het ICT-budget).
5. Ik zorg dat de organisatie richtlijnen heeft voor de beveiliging, o.a. over mobiel werken, de toegang tot systemen en het gebruik en beveiligen van usb-sticks en andere opslagmedia.
6. Ik zorg dat ICT-systemen en netwerken van de organisatie goed beveiligd en up-to-date zijn en blijven.
7. Ik zorg dat het netwerk in de organisatie continu gemonitord wordt, zodat verdachte situaties snel worden opgemerkt en de verantwoordelijken snel kunnen reageren op incidenten.
8. De organisatie laat de beveiliging regelmatig testen en oefent de procedures periodiek.
9. De organisatie zorgt voor medewerkers die bewust zijn van cyberrisico's en in hun werk rekening houden met cyberrisico's. Ik geef als bestuurder zelf het goede voorbeeld.
10. Ik zorg dat de organisatie een plan heeft wat te doen bij een cyber incident, ook waar het gaat om communicatie naar buiten de organisatie. Ik weet wie verantwoordelijk is en wie de besluiten mag nemen. Ik heb een procedure voor het op de juiste wijze melden van incidenten.

Zet cybersecurity periodiek op de bestuursagenda, maak deze vuistregels meetbaar voor de directie en toets regelmatig de stand van zaken met de organisatie. Laat experts de directie informeren.