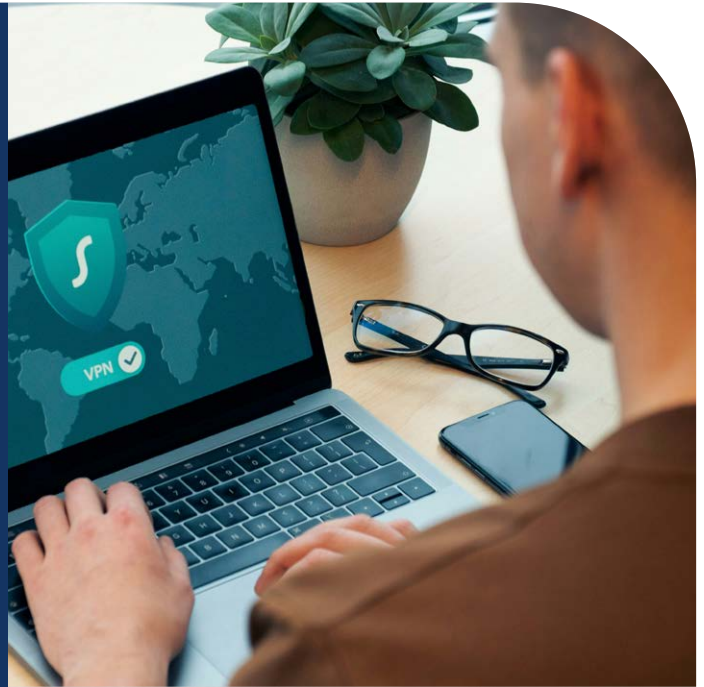


Burgemeesters en wethouders aan de slag met de Cyberbeveiligingswet



De nieuwe Cyberbeveiligingswet (Cbw) is een belangrijke stap in het versterken van de digitale veiligheid en weerbaarheid van gemeenten. Deze wet brengt aanzienlijke veranderingen met zich mee. Hoe gaat u hier als burgemeester of wethouder mee om?

Het is belangrijk om te begrijpen wat u als bestuurder zelf kunt doen, en wat u van de gemeentelijke organisatie mag verwachten om de Cbw succesvol te implementeren.

Raadsleden hebben ook een belangrijke rol bij het versterken van de informatiebeveiliging van hun gemeenten. Lees wat raadsleden kunnen doen: [raadsleden-en-informatiebeveiliging.pdf](#)

Rol burgemeesters en wethouders

Begrijp de wetgeving

Burgemeesters en wethouders moeten zich verdiepen in de Cbw om te begrijpen welke verplichtingen en verantwoordelijkheden deze met zich meebrengt.

Leer

De Cbw stelt een training over informatiebeveiliging voor burgemeesters en wethouders verplicht. Een dergelijke training helpt u om de juiste vragen te

stellen aan de organisatie, om de voorgestelde beveiligingsmaatregelen af te kunnen wegen.

De VNG raadt aan om (nog) geen trainingen te volgen van commerciële partijen, omdat de eisen nog niet zijn vastgesteld. Zodra deze duidelijk zijn, krijgt u nog 2 jaar de tijd voor het volgen van een training.

Informeer naar interne en externe risico's

Laat u regelmatig informeren over de stand van zaken van de informatiebeveiliging, bijvoorbeeld door de CISO en de proceseigenaren. Ook buiten het gemeentehuis is steeds meer gemeentelijke apparatuur en smart technology aanwezig, denk hierbij aan camera's of sluizen. Spreek daarom ook met de beleidsadviseur Openbare Orde en Veiligheid of andere betrokken adviseurs die zicht hebben op de (cyber)risico's in de openbare ruimte.

Laat risico's vastleggen

Geef de opdracht om cyberrisico's voor de gemeente vast te leggen op hetzelfde niveau als financiële, reputatie en juridische risico's. Dit kan in de P&C documenten. Hierdoor draagt u eraan bij dat digitale risico's als een integrale bestuurlijke verantwoordelijkheid worden gezien.

Reserveer voldoende medewerkers en middelen

Bespreek in het college en met de raad: Hebben we voldoende mensen en middelen beschikbaar voor de implementatie van de wet? Prioriteer. Gemeenten hebben het financieel zwaar, maar bezuinigingen op (digitale) veiligheid zijn onverstandig en kunnen later juist voor extra hoge kosten zorgen.

Help als burgemeester en wethouder de ambtelijke organisatie:

Vraag actief om cyberrisicoanalyses

Vraag naar actuele cyberrisicoanalyses, zowel binnen de organisatie, in de gemeentelijke (buiten) ruimte, als in de toeleveringsketen en bij partijen waarmee de gemeente samenwerkt. Daarmee ondersteunt u de prioritering van beveiligingsmaatregelen en het minimaliseren van risico's.

Stuur op werken volgens de Baseline Informatiebeveiliging Overheid (straks de BIO2)

Als college kunt u sturen op het structureel toepassen van de BIO door dit expliciet terug te laten komen in de beleidsstukken, werkprogramma's en collegeprioriteiten. Vraag als college ook aandacht voor de plan-do-check-act-cyclus.

Gebruik de ENSIA-rapportage strategisch

De jaarlijkse rapportage op basis van de ENSIA-methode in het voorjaar is hét verantwoordingsinstrument over de staat van informatiebeveiliging. Deze geeft ook steeds meer inzicht in de feitelijke veiligheid en helpt de organisatie te verbeteren. Behandel de ENSIA-rapportage niet alleen als een technische verantwoording, maar ook als bestuurlijk onderwerp. Vraag uw CISO en/of ENSIA-coördinator een toelichting op het rapport en bespreek wat nodig is om in control te blijven. Dit helpt ook om richting raad en rijksoverheid aan te tonen dat uw gemeente voldoet aan de zorgplicht van de Cbw.

Stel kaders voor monitoring en meldprocedures vast

Stel procedures vast voor het monitoren van cyberbeveiligingsincidenten en het melden van informatiebeveiligingsincidenten. Dit helpt uw organisatie bij het snel reageren op incidenten en het beperken van schade.

Stimuleer de implementatie van een ISMS

Ondersteun de inrichting van een Information Security Management System (ISMS), door hiervoor middelen en capaciteit beschikbaar te stellen. Werken volgens een ISMS-systematiek helpt bij het in kaart brengen van cyberrisico's, het effectief implementeren van beheersmaatregelen en het continu monitoren van de voortgang.

Maak bewustwording en training van medewerkers belangrijk

Zet in op een organisatiebrede leercultuur waarin informatiebeveiliging ook thuishoort. Stimuleer regelmatige trainingen, bewustwordingscampagnes en geef als burgemeester en wethouder het goede voorbeeld.

Voor vragen over dit document kunt u terecht bij teamadv@vng.nl