Samenvatting richtlijn netwerk- en informatiebeveiliging

De voorgestelde richtlijn beoogt een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging te waarborgen. Lidstaten worden verplicht hun paraatheid te verbeteren en beter met elkaar samen te werken. Exploitanten van kritieke infrastructuur, essentiële aanbieders van informatiemaatschappijdiensten en overheden krijgen de verplichting opgelegd adequate maatregelen te nemen om beveiligingsrisico's te beheren en ernstige incidenten aan de nationale bevoegde autoriteiten te rapporten. Het voorstel wordt gepresenteerd samen met de Strategie inzake cyberbeveiliging van de Europese Unie (zie dossier E130010) en vormt daarvan de kernactie. Achtergrond van het voorstel is het groeiende aantal beveiligingsincidenten met informatiesystemen. Omdat deze systemen geen grenzen kennen, kunnen ingrijpende verstoringen in één lidstaat ook voelbaar worden in andere lidstaten en in de Europese Unie als geheel.

Het bestaande beveiligingsniveau is gebaseerd op vrijwilligheid en dit biedt onvoldoende bescherming. Bovendien verschilt het capaciteits- en paraatheidsniveau sterk van lidstaat tot lidstaat. Omdat informatiesystemen grensoverschrijdend zijn, is het netwerk- en informatiebeveiligingsniveau maar net zo sterk als dat van de lidstaat met het laagste beschermingsniveau. Op grond van de geldende Europese regelgeving zijn alleen telecommunicatiebedrijven verplicht risicobeheermaatregelen te nemen en ernstige incidenten te rapporteren. Echter, ook andere sectoren die kritieke infrastructuur beheren of essentiële diensten leveren zijn sterk afhankelijk van correct werkende informatiesystemen, zoals banken, de energiesector, de gezondheidszorg en de overheid.

Het richtlijnvoorstel verplicht lidstaten in de eerste plaats een minimale nationale capaciteit te bewerkstelligen door voor netwerk- en informatiebeveiliging bevoegde autoriteiten aan te wijzen, computercrisisteams op te zetten (CERT's = Computer Emergency Response Teams) en nationale netwerk- en informatiebeveiligingsstrategieën en samenwerkingsplannen op te stellen. Verder moeten de bevoegde nationale autoriteiten samenwerken in het kader van een netwerk dat beveiligde en doeltreffende coördinatie, inclusief gecoördineerde informatie-uitwisseling, en detectie en reactie op EU-niveau mogelijk maakt. Ten slotte beoogt de richtlijn de ingang van een cultuur van risicobeheer en de onderlinge uitwisseling van informatie tussen particuliere en openbare sector.