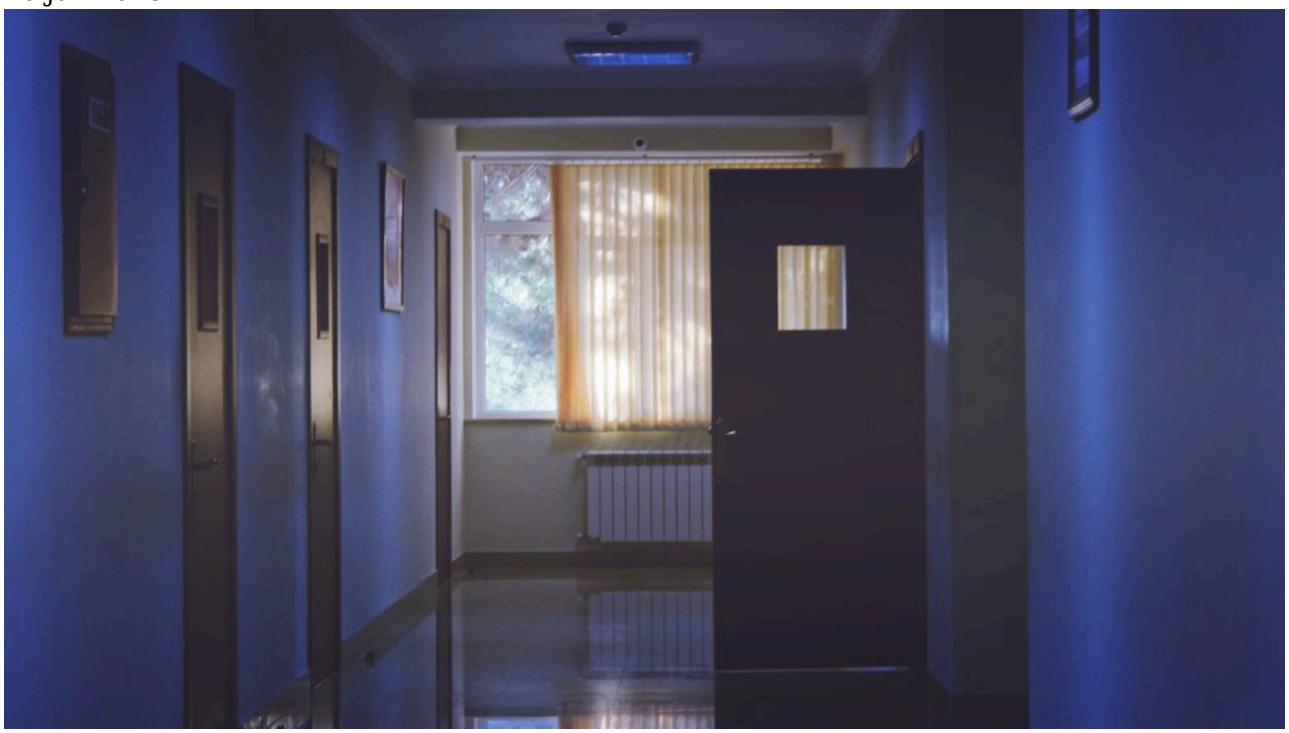
Ziekenhuizen volgens Cybersecuritywet geen essentiële dienst

10 juli 2018



De Cybersecuritywet verplicht aanbieders van essentiële diensten zoals drinkwaterbedrijven, banken en energiebedrijven verplicht om aan beveiligingseisen te voldoen. Zo moeten ze ‘adequate maatregelen’ nemen tegen inbreuken van buitenaf op hun netwerk- en informatiebeveiliging. Nieuw is verder dat ernstige cyberincidenten voortaan ook gemeld moeten worden bij de relevante toezichthouder (voor banken bijvoorbeeld DNB).

Ziekenhuizen geen ‘essentiële dienst’

Omdat ziekenhuizen niet als essentiële dienst worden aangemerkt, kwamen er vragen van de vaste commissie voor Volksgezondheid zorgde. In zijn uitleg waarom dit het geval is, wijst Bruins naar de criteria die gelden voor het beoordelen van vitale processen. Een proces in de samenleving wordt als vitaal beschouwd wanneer uitval leidt tot meer dan 5 miljard euro schade of een 1,0 procent daling van het reëel inkomen, meer dan 1.000 doden, ernstig gewonden of chronisch zieken, of wanneer meer dan 100.000 personen emotionele problemen of ernstig maatschappelijke overlevingsproblemen ondervinden.

‘Wij zijn destijds tot de conclusie gekomen dat er geen situaties zijn waarin uitval van ICT-systemen of -structuren in de zorg deze gevolgen zullen hebben. In Nederland is er namelijk geen centrale vitale technische infrastructuur voor de gehele zorg die bij uitval dergelijke gevolgen heeft voor landsbrede zorg,’ stelt Bruins. ‘Instellingen zijn zelf verantwoordelijk voor de veiligheid van informatievoorziening en -veiligheid.’

Bij uitval niet hele zorg getroffen

Mocht een deel van de zorg uitvallen, dan kan deze zorg volgens de minister in veel gevallen worden overgenomen door andere zorgaanbieders. Daarom heeft VWS geen processen in de zorg als vitaal geïdentificeerd en zijn er dus geen aanbieders van essentiële diensten aangewezen, aldus Bruins.

Hij merkt verder op dat de informatievoorziening en gegevensuitwisseling in de zorg van groot belang is voor de patiëntveiligheid en er daarom wordt ingezet op andere maatregelen om de veiligheid van de technische infrastructuur in de zorg te verhogen, zoals het opstellen van specifieke normen en het oprichten van een Computer Emergency Response Team voor de Zorg (Z-CERT).

Een andere maatregel is het Actieplan Informatiebeveiliging, dat is belegd bij Z-CERT. Het Actieplan, dat focust op bewustwording rond informatiebeveiliging in de zorgsector en ontwikkelt activiteiten ontwikkelt om die bewustwording naar een structureel hoger niveau te brengen.

Over de Cybersecuritywet

De nieuwe Cybersecuritywet is in februari van dit jaar aan de Tweede Kamer aangeboden. Hij moet dit jaar nog van kracht worden. Volgens de huidige Wet gegevensverwerking en meldplicht cybersecurity (Wgmc) zijn aanbieders van bepaalde diensten alleen verplicht dit soort incidenten te melden bij het Nationaal Cyber Security Centrum (NCSC) – dat voor Nederland fungeert als Cyber Security Incident Response Team (CSIRT). oewel de Wgmc al verplicht tot het melden van ernstige cyberincidenten, voldoet Nederland daarmee maar voor een deel aan de NIB-richtlijn. Toegevoegd in de nieuwe wet zijn de meldplicht bij de toezichthouder, de beveiligingseisen en de sancties die de toezichthouder kan opleggen.