# CHECKLIST

## Handreiking cybersecurity voor de bestuurder

U wilt aan de slag met cybersecurity om uw organisatie zo digitaal veilig mogelijk te maken. Onderstaande checklist helpt u uw organisatie weerbaar te maken. Het geeft u handvatten om uw organisatie voor te bereiden op een cyberincident, de schade ervan te beperken en de herstelcapaciteit te vergroten. De lijst is niet uitputtend en dient per organisatie verder te worden uitgewerkt.

### Zijn we voldoende voorbereid op een cyberincident?

- ☐ Hebben we voldoende en juist gekwalificeerd personeel om de cyberweerbaarheid van de organisatie te garanderen? Is ons personeel voldoende getraind om poortwachter te zijn?
- ☐ Zijn we voldoende voorbereid op digitale uitval en/of ontwrichting?
- ☐ Hebben we zicht op welke zorgplichten voor onze organisatie van toepassing zijn? Hebben we de juiste maatregelen getroffen om aan onze zorgplichten te voldoen?
  *Toelichting: u kunt hiervoor gebruikmaken van de CSR handreiking 'Ieder bedrijf heeft digitale zorgplichten, een handreiking voor bedrijven op het gebied van cybersecurity'. Deze handreiking biedt inzicht in de complexe wet- en regelgeving rondom zorgplichten op het vlak van cybersecurity en bevat tevens een checklist.*
- ☐ Hebben we het gewenste veiligheidsniveau bepaald ten aanzien van de risico's die we lopen? En hebben we dit veiligheidsniveau bewust gekozen? Oftewel: wat is onze 'risk appetite' in het digitale domein?
- ☐ Hebben we voldoende en juist geïnvesteerd, georganiseerd en geëquipeerd om dit gewenste veiligheidsniveau te bereiken en te handhaven?
  *Toelichting: Een maatstaf is om structureel 10 procent van het IT-budget te investeren in cybersecurity.*[10]
- ☐ Hebben we voor ogen welke processen en systemen van vitaal belang zijn en worden deze voldoende gemonitord? Wat zijn de 'kroonjuwelen' die we willen beschermen?
- ☐ Zijn we voldoende in staat om forensisch onderzoek dat wellicht plaats moet vinden als gevolg van het incident, niet te verstoren? Weten we hoe te handelen om sporen te behouden?
- ☐ Hebben we de juiste standaarden en richtlijnen ingevoerd binnen onze organisatie?
- ☐ Versterken de gekozen standaarden elkaar? Willen we ons laten certificeren?
- ☐ Vinden er voldoende interne en externe audits plaats? Maken we er gebruik van en voeren we de verbeterpunten door?
- ☐ Zijn we voldoende aangesloten bij andere lopende initiatieven die veiligheid kunnen bevorderen, zoals het Nationaal Detectie Netwerk (NDN), Information Sharing and Analysis Centres (ISAC's),het Digital Trust Centre (DTC) of een cyberweerbaarheidsnetwerk?
  *Toelichting: Het NDN is een netwerk van organisaties in de vitale sector die elkaar alerteren op onder andere kwetsbaarheden, malware en aanvallen. Dit netwerk zorgt voor het beter en sneller waarnemen van digitale gevaren en risico's. Door het (anoniem) delen van dreigingsinformatie kunnen de deelnemers gepaste maatregelen nemen om mogelijke schade te voorkomen of te beperken.*
  *Toelichting: ISAC's organiseren per vitale sector regelmatig bijeenkomsten van technische experts uit uw sector, de AIVD, de Nationale Politie en het Nationaal Cyber Security Centrum. Tijdens deze bijeenkomsten wordt er op basis van geheimhouding mondeling (veelal operationele) informatie gedeeld over cybersecurity-onderwerpen. Dit stelt alle partijen in de sector in staat gepaste maatregelen te nemen en mogelijke schade te voorkomen of te beperken.*
- ☐ Hebben we een beleid voor Coordinated Vulnerability Disclosure (CVD) ingevoerd? Is er voldoende capaciteit beschikbaar om de CVD af te handelen?
  *Toelichting: Coordinated Vulnerability Disclosure biedt ethische hackers de mogelijkheid ontdekte kwetsbaarheden te melden. Organisaties bieden daarbij de mogelijkheid om de kwetsbaarheid (anoniem) te melden op hun website. De organisatie is verplicht de kwetsbaarheid te verhelpen en de melder hiervoor te bedanken.*
- ☐ Beproeven we onze (digitale) beveiliging periodiek (bijv. jaarlijks) met een 'cyberoefening', evalueren we de uitkomsten en implementeren we de gewenste aanpassingen?
- ☐ Brengen we het onderwerp cybersecurity voldoende onder de aandacht van het personeel? Doen we voldoende aan (awareness)training van het personeel?
- ☐ Zijn onze fysieke en digitale beveiliging waar mogelijk aan elkaar gekoppeld?

### Zijn we voldoende in staat om een calamiteit het hoofd te bieden?

- ☐ Hebben we een goed functionerende crisisstructuur, inclusief escalatiemanagement en crisiscommunicatie met de woordvoeringslijn?
- ☐ Hebben we voor ogen welke groepen (keten)partners door incidenten kunnen worden geraakt en informeren we deze groepen tijdig en juist?
- ☐ Hebben we goed voor ogen welke partijen ons kunnen bijstaan bij het oplossen van cyberincidenten en hebben we goed contact met ze?
- ☐ Moeten we een cyberverzekering afsluiten?
- ☐ Voldoen wij aan wet- en regelgeving, zoals de Algemene verordening gegevensbescherming (AVG)[11] en de Wet beveiliging netwerk- en informatiesystemen (Wbni)[12]?

### Zijn we voldoende in staat om van een calamiteit te herstellen?

- ☐ Hebben we onze herstelprocedures op orde en is dit onderdeel van ons Business Continuity Plan en/of Disaster Recovery Plan?
- ☐ Hebben we onze nazorg inclusief interne en externe communicatie op orde?
- ☐ Hebben we een goed evaluatieproces ingericht met het oog op 'lessons learned' en het doorvoeren van aanpassingen?
- ☐ Hebben we een proces ingericht dat zorgt voor aangifte bij de politie?

10 Verhagen, H. (2016), De economische en maatschappelijke noodzaak van meer cybersecurity, Nederland digitaal droge voeten, Den Haag

11 https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679

12 https://wetten.overheid.nl/BWBR0041515/2019-01-01

CSR Cyber Security Raad