CSR Cyber Security Raad

HANDREIKING CYBERSECURITY VOOR DE BESTUURDER

CYBERSECURITY OP STRATEGISCH NIVEAU

Onze samenleving digitaliseert in sneltreinvaart. Daar plukken we de vruchten van. Ons land is een belangrijke kenniseconomie en digitale haven. Maar we ondervinden ook nadelen. Zo worden persoonsgegevens, banktegoeden en bedrijfsgevoelige informatie gestolen, vindt identiteitsfraude plaats en verstoren kwaadwillenden onze vitale processen.[1]

De samenleving verwacht dat organisaties hun digitale dienstverlening op orde hebben. Vooral vitale processen en de infrastructuur moeten beschermd zijn tegen (digitale) dreigingen. Niemand wil dat de maatschappij ontwricht raakt door een cyberincident. Van publieke en private organisaties in de zogenoemde ‘vitale sectoren’ wordt dan ook verwacht dat ze weerbaar en veerkrachtig zijn op het moment dat zich een incident voordoet.

Een goede cybersecurity-aanpak raakt alle elementen in uw organisatie: in de hoogte (organisatiestructuur) en in de breedte (dienstverlening). Het is daarom bij uitstek een strategische uitdaging voor de boardroom. Uw IT-afdeling speelt uiteraard ook een belangrijke rol, maar u bent degene die op strategisch niveau de kaders bepaalt voor het formuleren, implementeren, bewaken en handhaven van het cybersecuritybeleid in uw organisatie. Dat is overigens geen eenmalige exercitie, maar een continu proces.

De impact van cyberincidenten wordt steeds groter. Ze hebben niet alleen gevolgen voor uw organisatie en uw ketenpartners, maar kunnen ook persoonlijke gevolgen voor u hebben. Dit kunt u lezen in de CSR handreiking 'Ieder bedrijf heeft digitale zorgplichten, een handreiking voor bedrijven op het gebied van cybersecurity'. Digitale weerbaarheid vraagt én verdient daarom dezelfde aandacht als bijvoorbeeld de financiële en operationele gezondheid van uw organisatie.

Met behulp van deze handreiking krijgt u inzicht in hoe u cybersecurity kunt beleggen binnen uw organisatie.

Namens de Cyber Security Raad,

Jos Nijhuis, covoorzitter
Dick Schoof, covoorzitter

Cybersecurity is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan. De schade kan bestaan uit: aantasting van de betrouwbaarheid van ICT, beperking van de beschikbaarheid en schending van de vertrouwelijkheid en/of integriteit van de in ICT opgeslagen informatie en de herkomst hiervan.

1 Vitale processen zijn processen die bij uitval of verstoring tot ernstige maatschappelijke ontwrichting kunnen leiden. Voorheen werd ook wel gesproken van vitale sectoren. Omdat niet alle processen binnen een sector vitaal zijn, ligt de focus nu op de vitale processen in plaats van sectoren als geheel. Het identificeren van vitale processen maakt het mogelijk om instrumenten en schaarse middelen meer efficiënt en gericht in te zetten. (bron: NCTV)

HANDREIKING CYBER-SECURITY VOOR DE BESTUURDER

Het belang van cybersecurity in de vitale sectoren

Als bestuurder wilt u inspelen op de kansen die u ziet voor uw organisatie en wilt u de mogelijke gevolgen van incidenten tot een aanvaardbaar risico beperken. Een goed cybersecuritybeleid biedt de mogelijkheid om beide doelstellingen te realiseren. Daarom past het bij uw rol als bestuurder om hierop actie te ondernemen. Dit vergt echter soms een andere aanpak dan u gewend bent bij uw andere verantwoordelijkheden. Met behulp van deze handreiking, opgesteld door de Cyber Security Raad, krijgt u inzicht in hoe u cybersecurity in uw organisatie kunt beleggen.

Welke afwegingen maakt u in het kader van cybersecurity?

Om te komen tot een goede cybersecurity-aanpak is het van belang dat u zicht heeft op de risico's die uw organisatie loopt. Vervolgens maakt u op basis daarvan risicogebaseerde afwegingen. En tot slot geeft u sturing aan het proces dat u opstart om te komen tot een (digitaal) veiliger organisatie.

Actueel inzicht in risico's

Weet u wat uw belangrijkste assets ('kroonjuwelen') zijn? Ofwel: wat is zo kostbaar en belangrijk voor uw organisatie dat niemand anders het in handen mag krijgen? En hoe beschermt u dit? Waartegen? Voor u als bestuurder is het relevant om te weten waar de grootste dreigingen vandaan komen. U kunt dan juiste maatregelen nemen. Het mag duidelijk zijn dat honderd procent veiligheid niet bestaat en dat eindeloos investeren in cybersecurity geen reële optie is. Een maatstaf is om structureel 10 procent van het IT-budget te investeren in cybersecurity.[2]

De CEO van Target - een grote warenhuisketen in onder andere Amerika en Australië - stapte op nadat de creditcardgegevens van klanten door online diefstal in handen kwamen van cybercriminelen. Daaruit blijkt dat veiligheids- en privacy-incidenten grote gevolgen hebben voor de CEO en het imago van een bedrijf. Redenen genoeg om cybersecurity op de agenda van de boardroom te zetten.

Risicogebaseerde afwegingen

Er kan ogenschijnlijk een spanningsveld ontstaan tussen enerzijds de economische belangen en/of de publieke functie van uw organisatie en anderzijds de (digitale) veiligheid van uw organisatie. Echter, zij gaan hand in hand. Een cybersecurity-incident kan zo'n grote impact op uw organisatie hebben, en potentieel ook op uw (keten)partners, dat het vanuit zijn aard

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

direct de economische belangen en de veiligheid van uw organisatie raakt. De vraag is waar u de focus op legt. Waar investeert u vooral in? Maar ook: welke risico's accepteert u? Per definitie moet u keuzes maken en zaken tegen elkaar afwegen. Zorg ervoor dat u structureel beschikt over relevante informatie, zodat u risicogebaseerde afwegingen kunt blijven maken.

Hoe belegt u cybersecurity in uw organisatie?

Het structureel kunnen beschikken over relevante informatie voor uw risicogebaseerde afwegingen en besluiten, is een resultante van de wijze waarop u cybersecurity in uw organisatie belegt. Hieronder geven we u een opsomming van mogelijke functies die u kunnen helpen bij het beleggen van heldere taken en verantwoordelijkheden.

De precieze vorm en benaming van de functies kunnen verschillen per organisatie. Ook heeft de omvang van de organisatie invloed op de taakverdeling. In sommige (kleinere) bedrijven worden meerdere taken bij één persoon ondergebracht. Hierbij is het van belang dat er geen conflicterende belangen ontstaan en dat er gelet wordt op functie-scheiding daar waar dat nodig is. Het verdient aanbeveling om de hoogste functionaris die belast is met security, een onafhankelijke positie te geven.

De Chief Information Security Officer (CISO) heeft een essentiële adviserende rol richting het bestuur en is belast met het formuleren en bewaken van het fysieke en digitale informatiebeveiligingsbeleid. De CISO zou dan ook onafhankelijk binnen de eigen organisatie moeten opereren en direct aan de Raad van Bestuur rapporteren. Soms is de CISO-rol belegd bij de Chief Risk Officer (CRO). In dat geval heeft de CRO naast andersoortige risico's ook de digitale veiligheidsrisico's in portefeuille.

De Chief Information Officer (CIO) is verantwoordelijk voor het ontwikkelen en beschikbaar stellen van digitale middelen aan de rest van de organisatie. Deze functionaris heeft een sleutelrol met betrekking tot cybersecurity en moet in staat zijn onafhankelijk te adviseren. In een aantal organisaties maakt de CIO onderdeel uit van de Raad van Bestuur.

De Functionaris voor de gegevensbescherming (FG). Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf dit moment kunnen organisaties verplicht zijn een FG aan te stellen. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de AVG. De AVG vervangt de Wet bescherming persoonsgegevens (Wbp).

De Raad van Commissarissen (RvC) of Raad van Toezicht (RvT) heeft een controlerende en adviserende rol. Het is zijn taak de Raad van Bestuur strategisch te adviseren over digitale veiligheid en te controleren op dit thema. Niet iedere RvC of RvT is hiervoor voldoende geëquipeerd. Extra toerusting valt dan aan te bevelen, om zo het onderwerp cybersecurity tot op het hoogste niveau in de organisatie te beleggen.

Hoe bouwt u structureel aan digitale veiligheid?

Versterk het bestuur

- Neem uw verantwoordelijkheid voor digitale weerbaarheid.
  Dit betekent dat u leiderschap toont bij het formuleren, implementeren en handhaven van het cybersecuritybeleid. Dit is geen eenmalige exercitie. Het is een continu proces dat bestuurlijke aandacht nodig heeft.
- Benoem een portefeuillehouder in het bestuur.
  De portefeuillehouder en de CISO definiëren de doelen en kaders, faciliteren implementatie en bewaken de voortgang en handhaving van het cybersecuritybeleid. Daarmee zijn de overige bestuurders niet ontslagen van hun verantwoordelijkheden!
- Agendeer cybersecurity structureel op uw boardroomagenda.
  Werk op basis van een voor u begrijpelijke rapportage zodat u voldoende inzicht heeft in de weerbaarheid van uw organisatie.
- Zorg dat het kennisniveau van cybersecurity bij alle leden van de Raad van Bestuur op het gewenste basisniveau is.
  Cybersecurity is een aparte discipline met zijn eigen begrippen en taalgebruik. Daarom is het van belang te zorgen voor voldoende basis- kennis bij uw bestuursleden, zodat zij elkaar, de CISO en andere experts scherp kunnen houden.
- Creëer als bestuur een open sfeer in uw organisatie. Medewerkers moeten zich vrij voelen misstanden te melden. Het gebruik van gedragsregels binnen uw organisatie kan u hierbij helpen. Geef zelf daarbij het goede voorbeeld.
- Zorg dat cybersecurity een regelmatig terugkerend onderwerp van gesprek is met uw ketenpartners en leveranciers. De keten is zo sterk als de zwakste schakel. Neem bepalingen over cybersecurityniveaus van processen, producten, diensten en medewerkers op in uw overeenkomsten. Maak daarin ook afspraken over hoe te handelen bij incidenten. Wanneer u regelmatig overlegt, helpt u dit onderwerp op de agenda te houden. Bewustwording en veilig gedrag nemen daardoor toe.
- Maak gebruik van de checklist die bij deze handreiking hoort. Het geeft u goede handvatten om uw organisatie zo digitaal veilig mogelijk te maken. Daarnaast kunt u ook 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.
- Cybersecurity is opgenomen in de herziene Nederlandse Corporate Governance Code (CGC).[3] U bent degene die op strategisch niveau de kaders bepaalt. Voor de invulling van cybersecurity kunt u gebruikmaken van de 'Advancing Cyber Resilience, Principles and Tools for Boards' van het World Economic Forum (WEF).[4]

DigiNotar was een van oorsprong Nederlands bedrijf dat zogenaamde SSL-certificaten uitgaf. Deze certificaten dienden ter identificatie van websites en beveiliging van webverkeer. DigiNotar is in 2011 gehackt en er zijn tientallen frauduleuze certificaten aangemaakt. DigiNotar heeft het feit dat zij gehackt was enige tijd stilgehouden.
De gevolgen van de hack waren enorm. De nationale veiligheid kwam in het geding, omdat het vertrouwen in alle DigiNotar-certificaten werd opgezegd. Dit resulteerde onder andere in onbereikbare websites, omdat Google en anderen automatisch dubieuze certificaten opzeggen. Het bedrijf DigiNotar bestaat niet meer.

3 https://www.mccg.nl/download/?id=3364

4 https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards

Insider threat
Uw medewerkers dienen betrouwbaar te zijn. Zij hebben in meer of mindere mate toegang tot belangrijke informatie. U kunt bij de indiensttreding van uw kandidaat vragen om een Verklaring Omtrent Gedrag (VOG) te overleggen. Tijdens het dienstverband kunt u uw personeel (periodiek) screenen. Zorg dat de medewerkers de juiste autorisaties hebben op basis van hun rollen en taken. En als die rollen en taken wijzigen, behoren de autorisaties ook te wijzigen. Bij medewerkers die vertrekken worden alle autorisaties direct ingetrokken en wachtwoorden gewijzigd. Niet alleen hun eigen wachtwoorden, maar ook van algemene systemen waar zij toegang toe hadden. Hiermee voorkomt u dat ongewenste situaties ontstaan.

Daarnaast dient u ervoor te zorgen dat medewerkers op regelmatige basis bewust worden gemaakt (en gehouden) van de spelregels ten aanzien van cybersecurity en hoe te handelen bij incidenten.

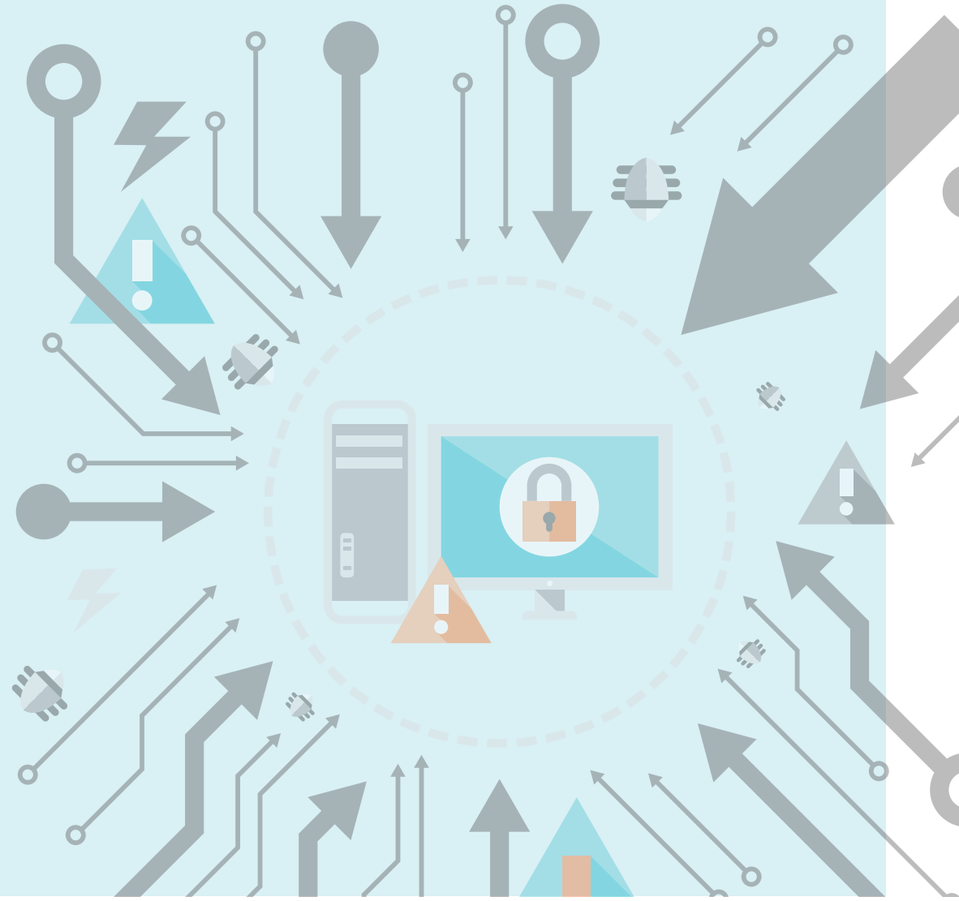
Veiligheid in de keten
Een solide cybersecurity-aanpak heeft niet alleen betrekking op uw eigen organisatie, maar omvat ook uw keten van leveranciers, (onder)aannemers, afnemers en voor zover relevante eindgebruikers. De onderlinge digitale verwevenheid en afhankelijkheid van al deze partijen neemt namelijk steeds verder toe. Daarmee neemt ook de potentiële impact van een cyberincident toe. Bestuurders of andere functionarissen die belast zijn met cybersecurity bij uw ketenpartners, zijn daarom belangrijke gesprekspartners voor u. Overleg regelmatig met elkaar over digitale veiligheid in de keten. Het verdient aanbeveling om relevante informatie over digitale kwetsbaarheden binnen uw sector open met elkaar te delen. Daardoor kan iedere organisatie in de keten passende maatregelen nemen. Regelmatig overleg zorgt er ook voor dat cybersecurity als onderwerp hoog op de agenda blijft staan. Bewustwording en veilig gedrag nemen daardoor toe.

Als niet-vitale organisatie kunt u zich aansluiten bij het Digital Trust Centre (DTC). Het DTC heeft als taak bedrijven betrouwbare en onafhankelijke informatie te verschaffen over digitale kwetsbaarheden, het geven van concrete handelingsadviezen en het stimuleren van samenwerkingsverbanden op het vlak van cybersecurity tussen bedrijven onderling.

Nationale veiligheid
Wanneer uw organisatie een vitaal proces uitvoert, kan verstoring of uitval daarvan mogelijk tot maatschappelijke ontwrichting leiden en/of de nationale veiligheid in gevaar brengen. Bedrijfscontinuïteit is dan een extra grote verantwoordelijkheid.
Het voorkomen van een cyberincident en het adequaat reageren als zich toch een incident voordoet, behoren dan ook tot uw dagelijkse bedrijfsvoering.

Afstemmen fysieke en digitale veiligheid
Het is niet altijd vanzelfsprekend dat cybersecurity in een organisatie is ingebed. En als dat wel het geval is, blijkt dat niet altijd op hetzelfde hoge niveau te zijn als de fysieke beveiliging. Ook zijn digitale en fysieke veiligheid lang niet altijd goed op elkaar afgestemd. De voordeur zwaar bewaken terwijl de 'digitale' achterdeur wagenwijd openstaat, helpt u niet om uw organisatie veilig te krijgen. Laat beide afdelingen samenwerken op de terreinen die ze gemeenschappelijk hebben.

Gebruik checklist
U wilt aan de slag met cybersecurity om uw organisatie zo digitaal veilig mogelijk te maken. Daarom hebben we in deze handreiking een checklist opgenomen. Daarmee helpt u uw organisatie digitaal 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.



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 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.[5]
- ☐ 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 aangesloten op het Nationaal Detectie Netwerk (NDN)?
  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.
- ☐ Zijn we voldoende aangesloten bij andere lopende initiatieven die veiligheid kunnen bevorderen, zoals Information Sharing and Analysis Centres (ISAC's) of het Digital Trust Centre (DTC)?
  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 Responsible Disclosure (RD) ingevoerd? Is er voldoende capaciteit beschikbaar om de RD af te handelen?
  Toelichting: Responsible 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) en de Cybersecuritywet?

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?
- ☐ 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?

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

CSR Cyber Security Raad

De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het kabinet en het bedrijfsleven (via het kabinet) en is samengesteld uit hooggeplaatste vertegenwoordigers van publieke en private organisaties en de wetenschap. De raad is in 2011 door de toenmalige minister van Veiligheid en Justitie ingesteld. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen. De unieke samenstelling van de raad (publiek, privaat, wetenschap) maakt het mogelijk prioriteiten, knelpunten en kansen vanuit diverse invalshoeken te benaderen. De CSR heeft twee covoorzitters: één namens de publieke sector en één namens de private sector.

1e herziene druk, Den Haag, april 2018

CSR Cyber Security Raad