Cyber Security Assessment (CSA)

Toelichting

De CSA is ter ondersteuning van de manager en de IT-auditor bij het bepalen van de cyberrisico's van een organisatie.

Aanpak

Na het doorlopen van de onderstaande stappen, kan het cyberrisicoprofiel bepaald worden en kan gericht gezocht worden in beschikbare standaarden naar relevante maatregelen.

1. Bepaal de risico-indicatie per vraag met ja of nee op basis van het actuele beeld.
   Als een vraag niet kan worden beantwoord, dan is het antwoord in principe 'nee'.
2. Na beantwoording van alle vragen verschijnt in het dashboard de totale risicoscore (1 - 10) en relevante standaarden.
3. Bekijk de relevante standaard(en) voor specifieke maatregelen.

Vragen per categorie:

Indicatie voor laag risico ← → Indicatie voor hoog risico

Ja | Nee

Organisatie & Governance		Selecteer score (Ja of Nee)	Toelichting van invuller:
1	Staan cyberrisico's op de agenda van de directie?	Nee	
2	Is de verantwoordelijkheid voor cyberrisico's eenduidig en expliciet belegd binnen de organisatie?	Nee	
3	Is de organisatie in geringe mate afhankelijk van internet voor de bedrijfsvoering?	Ja	
4	Werkt de organisatie samen met deskundige externe partijen voor de bestrijding van cybercrime?	Nee	
5	Is (cyber)security een geïntegreerd onderdeel van de bedrijfsvoering?	Ja	
6	Leveren de processen voor beheersing van cybercrime een betrouwbaar en actueel beeld voor maatregelen tegen cyberrisico's?	Nee	
7	Heeft een directielid cybersecurity in zijn portefeuille?	Ja	
8	Heeft u een bestaand netwerk van cybersecurity contacten dat u in kan zetten in geval van cyberincidenten?	Nee	
	Totaal score	4	
Gedrag & Cultuur		Selecteer score (Ja of Nee)	Toelichting van invuller:
1	Zijn medewerkers op de hoogte van het belang van cybersecurity?	Nee	
2	Zijn in het afgelopen jaar awareness programma's t.a.v cybercrime uitgevoerd in de organisatie?	Ja	
3	Staan medewerkers positief tegenover een hoog niveau van beveiliging?	Ja	
4	Zijn awareness programma's algemeen of op concrete werksituaties gericht?	Ja	
5	Weten medewerkers waar zij incidenten moeten melden?	Nee	
6	Spreken medewerkers elkaar aan op onveilig gedrag?	Ja	
7	Wordt het effect van awareness programma's gemeten en worden incidenten gedeeld?	Ja	
8	Wordt het effect van awareness programma's gedeeld met relevante partijen?	Ja	
9	Wordt het effect van awareness programma's opgevolgd?	Ja	
10	Toont (senior) management voorbeeldgedrag t.a.v. cybercrime risico's?	Ja	
	Totaal score	8	
Waardeketen (stakeholders) versus risico's		Selecteer score (Ja of Nee)	Toelichting van invuller:
1	Heeft de organisatie een goed beeld van de belangrijkste assets (waardevolle doelen) voor de organisatie?	Nee	
2	Heeft de organisatie zicht op potentiële cyberdreigingen in relatie tot haar assets?	Ja	
3	Zijn alle interne stakeholders voor effectieve cybersecurity in kaart gebracht / beschikt de organisatie over een actuele stakeholdersanalyse?	Ja	
4	Zijn alle externe stakeholders voor effectieve cybersecurity in kaart gebracht / beschikt de organisatie over een actuele stakeholdersanalyse?	Ja	
5	Zijn de taken en verantwoordelijkheden van deze stakeholders goed afgestemd?	Ja	
6	Zijn partners in de business keten zich bewust van cybercrime risico's?	Ja	
	Totaal score	8	
Inzicht in technologielandschap		Selecteer score (Ja of Nee)	Toelichting van invuller:
1	Heeft de organisatie een compleet en actueel beeld van het technologielandschap dat gebruikt wordt voor de bedrijfsvoering?	Nee	
2	Heeft de organisatie een compleet en actueel beeld van de interne en externe technische koppelvlakken?	Ja	
3	Zijn bestaande kwetsbaarheden en de getroffen beveiligingsmaatregelen in het technologielandschap bekend?	Ja	

4	Wordt er opvolging gegeven aan (gedetecteerde) kwetsbaarheden in het technologielandschap?	Ja	
5	Staat u alleen door u zelf beheerde devices toe in het bedrijfsnetwerk?	Nee	
6	Zijn communicatiekanalen met klanten volledig in beeld?	Nee	
7	Wordt binnen de organisatie rekening gehouden met de life-cycle van belangrijke IT componenten?	Nee	
8	Is een proces ingericht om periodiek alle IT componenten in de IT infrastructuur, legaal en illegaal, in kaart te brengen?	Ja	
9	Worden het functioneren en gedrag van kritieke IT componenten bewaakt?	Ja	
	Totaal score	6	
Wet- en regelgeving		Selecteer score (Ja of Nee)	Toelichting van invuller:
1	Hebben veranderingen in wet- & regelgeving geen of beperkte invloed op de IT-omgeving van de organisatie?	Nee	
2	Heeft wet- & regelgeving een beperkte impact op processen / procedures bij de afhandeling van cyber-incidenten?	Ja	
3	Bestaan contacten met politie en/of justitie en/of NCSC over (mogelijke) cyber-incidenten?	Ja	
4	Is binnen de organisatie bekend welke wet- & regelgeving relevant is in het kader van cybercrime, bijvoorbeeld meldplicht datalekken, identiteitsfraude en aansprakelijkheid?	Ja	
5	Heeft de organisatie maatregelen genomen om risico's op datalekken af te dekken?	Ja	
6	Heeft de organisatie maatregelen genomen om risico's op identiteitsfraude af te dekken?	Ja	
	Totaal score	8	
Detectie		Selecteer score (Ja of Nee)	Toelichting van invuller:
1	Is de organisatie in staat om tijdig interne en externe cyberdreigingen te detecteren?	Nee	
2	Heeft de organisatie recent succesvol een cyberaanval afgeslagen?	Ja	
3	Wordt afwijkend gedrag van IT infrastructuur componenten gesignaleerd?	Ja	
4	Is (geautomatiseerde) detectie ingericht op incidenten / gebeurtenissen die duiden op cybercrime?	Ja	
5	Is samenwerking met externe partijen ingericht voor het detecteren van nieuwe bedreigingen?	Nee	
6	Wordt actief informatie uitgewisseld met externe partijen over actuele cybercrime dreigingen?	Nee	
7	Is een proces ingericht om signalen van inbreuken op fysieke en logische beveiliging af te handelen?	Nee	
8	Is een centraal punt in de organisatie beschikbaar en ingericht om inbreuken op de beveiliging af te handelen?	Ja	
	Totaal score	5	
Reactie		Selecteer score (Ja of Nee)	Toelichting van invuller:
1	Kan de organisatie snel acteren richting de diverse stakeholders in geval van een cyberdreiging?	Nee	
2	Is een specifiek proces ingericht voor de afhandeling van cybersecurity incidenten?	Ja	
3	Is een CSIRT of vergelijkbaar orgaan ingericht en aangesloten op de reguliere crisisorganisatie?	Ja	
4	Maakt de organisatie voor de afhandeling van incidenten onderscheid o.b.v. bijvoorbeeld impact van een incident?	Ja	
5	Vinden periodiek trainingen / testen plaats om cyberincidenten effectief af te handelen?	Ja	
6	Zijn leveranciers en afnemers onderdeel van het responseproces en zijn zij daarvan op de hoogte?	Ja	
7	Zijn leveranciers en afnemers betrokken bij de trainingen / testen voor cyberincidenten?	Ja	
	Totaal score	9	