Ministerie van Economische Zaken
en Klimaat

Deelnemersclassificatie

Onderscheid tussen deelnemers aan cybersecurity-informatiedeling

digital trust
center.

Waarom maken we onderscheid tussen deelnemers bij cybersecurity informatiedeling?

De organisaties die deelnemen aan een samenwerkingsverband verschillen in hun behoefte aan cybersecurity-informatie en hun vermogen om cybersecurity-informatie te gebruiken. Het gericht versturen van cybersecurity-informatie in een samenwerkingsverband vraagt daarom om een indeling van deelnemende organisaties met behulp van relevante kenmerken op basis waarvan cybersecurity-informatie gericht kan worden gedeeld. Deze factsheet geeft een mogelijke indeling van deelnemers weer die rekening houdt met informatiebehoefte en verwerkingscapaciteiten. Met behulp van deze indeling kunnen samenwerkingsverbanden en de aangesloten organisaties geïnspireerd worden om te kunnen bepalen welke informatie bij wie terecht moet komen.

Totstandkoming

Het overzicht van soorten cybersecurity-informatie en indeling is in samenwerking met het Cyber Weerbaarheidscentrum Brainport (CWB) en TNO ontwikkeld. Aanvullingen en wijzigingen voorbehouden.

Hoe is de deelnemersclassificatie ontstaan?

Bij de ontwikkeling van de deelnemersclassificatie stond de vraag centraal op welke manier deelnemers (van het CWB) kunnen worden ingedeeld om gericht van cybersecurity-informatie te worden voorzien. Voor het beantwoorden van deze vraag is in samenwerking met organisaties die betrokken waren bij de opstartfase van het CWB gekeken naar de kenmerken en behoefte aan cybersecurity-informatie.
De deelnemersclassificatie is ontwikkeld in een iteratief proces van interviews, werksessies, en simulatiesessies. In de interviews is de informatiebehoefte en informatieverwerkingscapaciteit van deelnemers onderzocht. Dit is verder uitgewerkt in een werksessie, waarna een longlist van deelnemerskenmerken is opgesteld. De longlist is verwerkt tot een gevalideerde shortlist met drie groepen aan kenmerken. In twee simulatiesessies is de indeling vervolgens getest met de deelnemende organisaties betrokken bij het CWB.

De deelnemersclassificatie

Tijdens de ontwikkeling van de deelnemersclassificatie is gebleken dat weinig op voorhand verwachte kenmerken (zoals de omvang van organisaties, de locatie of het soort intellectueel eigendom) daadwerkelijk relevant zijn voor het gericht delen van cybersecurity-informatie. Uit het onderzoek met de pilotdeelnemers van het CWB zijn drie specifieke kenmerken naar voren gekomen die helpen om informatie op maat te versturen. Deze kenmerken zijn:

1. De mogelijkheid tot inhoudelijke verwerking van cybersecurity informatie (waar kan een organisatie wat mee?)
    - Op welk organisatieniveau (strategisch/tactisch of /operationeel/technisch) is cybersecurity in de organisatie belegd?
    - Welke informatie is van toepassing op de organisatie?

2. De capaciteiten voor het verwerken van cybersecurity informatie (hoe verwerkt een organisatie cybersecurity informatie?)
    - Heeft de organisatie een Security Operations Center?
    - Maakt de organisatie gebruik van een Computer Security Incident Response Team?
    - Is de organisatie in staat cybersecurity informatie in de vorm van CVE/CVSS [1] te gebruiken?

3. De behoefte aan cybersecurity informatie (welke vragen heeft de organisatie?)
    - Zijn IT en IT-security in eigen beheer, of uitbesteed aan externe partijen[2]?

Tijdens het onderzoek is gebleken dat de mogelijkheid tot inhoudelijke verwerking van cybersecurity-informatie (het eerste kenmerk) als zeer (zo niet het meest) nuttig wordt ervaren voor het gericht versturen van cybersecurity-informatie. Het onderscheid tussen de organisatieniveaus waarop cybersecurity-informatie wordt verwerkt is bepalend voor het soort informatie waar een organisatie wat mee kan. Tegelijk is dit onderscheid in de praktijk soms lastig te maken. Een informatiebeveiligingsbeambte kan in kleine organisaties bijvoorbeeld op strategisch niveau beslissingen nemen terwijl CISO's van grote organisaties soms beperkt actief zijn op strategisch niveau. Samenwerkingsverbanden zullen bij de toetreding van een organisatie moeten bespreken op welk niveau de organisatie cybersecurity-informatie in de praktijk verwerkt. . Tevens is gebleken dat de operationele capaciteiten voor het verwerken van cybersecurity-informatie grotendeels bepalen welke informatie een organisatie wil ontvangen. Hoe operationele capaciteiten voor het verwerken van cybersecurity informatie kunnen worden beschreven en ingedeeld, is nog onderwerp van onderzoek[3] .

Gebruik van de indeling

De deelnemersclassificatie wordt door het CWB gebruikt om partijen in te delen die zich aanmelden als deelnemer. Op basis van deze indeling kan het CWB vervolgens de deelnemer adviseren welke soorten cybersecurity-informatie met de organisatie worden gedeeld. De kenmerken kunnen ook worden opgenomen in het profiel van de deelnemende organisatie zodat ze inzichtelijk zijn voor andere deelnemers.

De praktijk moet uitwijzen in hoeverre cybersecurity informatiedeling in het CWB volgens de kenmerken van de deelnemersclassificatie verloopt. Tijdens de simulatiesessies is gebleken dat het gebruik van de indeling gewenning vereist. Daarnaast zal de noodzaak voor het gebruik van een indeling toenemen naarmate er meer informatie wordt gedeeld en er een information-overload wordt ervaren. Ook wanneer de meerwaarde van het indelen van deelnemende organisaties aanvankelijk beperkt lijkt, adviseert TNO de kenmerken van nieuwe deelnemers aan een samenwerkingsverband structureel in kaart te blijven brengen, zodat deze later kunnen worden toegepast.

Contactgegevens

Cyber Weerbaarheidscentrum Brainport:
Marringa, R.J. (Robert-Jan)
marringa@24innovation.nl

Digital Trust Center:
Kolk, J.F. van der (Jacco)
J.F.vanderKolk@minezk.nl

TNO:
Krabbendam-Hersman, T.H.E.E.A. (Tjarda)
tjarda.krabbendam@tno.nl

[1] Het Common Vulnerability Scoring System (CVSS) is een gratis en open industriestandaard om de ernst van beveiligingslekken in de computerbeveiliging te beoordelen. Common Vulnerabilities and Exposures (CVE) is een lijst vermeldingen, elk met een identificatienummer, een beschrijving, referentie, etc.

[2] bij uitbesteding kan cybersecurity informatie nog steeds bruikbaar zijn met het oog op toezicht op leveranciers (supplier assurance).

[3] Binnen TNO en daarbuiten wordt onderzoek naar capaciteiten voor het verwerken van cybersecurity informatie uitgevoerd (onderdeel van een Shared Research Programma met financiële instellingen).

digital trust center.