Ministerie van Economische Zaken
en Klimaat

Soorten cybersecurity-informatie

digital trust
center.

Waarom een overzicht van soorten cybersecurity-informatie?
Cybersecurity-informatie is een verzamelterm waarmee wordt verwezen naar verschillende soorten informatie. Organisaties kunnen door de hoeveelheid informatie en de variatie in informatie snel overladen worden. Het is daarom belangrijk om onderscheid te maken tussen verschillende soorten cybersecurity-informatie. Deze factsheet geeft een overzicht van soorten cybersecurity-informatie en een manier waarop deze ingedeeld kan worden. De factsheet draagt bij aan het concretiseren van de behoefte of de beschikbaarheid van verzamelde en uitgewisselde informatie.

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 indeling ontstaan?
Bij het ontwikkelen van het overzicht en de indeling van soorten cybersecurity-informatie stond de vraag centraal op welke manier soorten cybersecurity-informatie onderscheiden kunnen worden, waarmee informatie gericht verzameld en uitgewisseld kan worden met de deelnemers van het CWB. Het overzicht en de indeling zijn ontwikkeld in een iteratief proces van interviews, werksessies en simulatiesessies. Tijdens de interviews en werksessies is uitgevraagd welke soorten cybersecurity-informatie gebruikt worden en waar deze informatie vandaan komt. Tevens is gevraagd over welke informatie organisaties zouden moeten beschikken om voldoende 'cybersecure' te opereren. De voorbeelden en resultaten zijn uitgewerkt en gevalideerd en aangevuld door organisaties die betrokken waren tijdens de opstartfase van het CWB. Het overzicht van soorten cybersecurity-informatie is vervolgens getest tijdens twee simulatiesessies.

Soorten cybersecurity- informatie
Het resultaat van het onderzoek en simulatiesessies is een overzicht van 19 soorten cybersecurity-informatie. Deze soorten cybersecurity-informatie zijn ingedeeld in vier clusters:

- Strategisch/tactisch gebruik ten behoeve van proactie en preventie;
- Strategisch/tactisch gebruik ten behoeve van incident respons;
- Operationeel/technisch gebruik ten behoeve van proactie en preventie;
- Operationeel/technisch gebruik ten behoeve van incident respons.

Bovenstaande indeling gecombineerd met de soorten cybersecurity-informatie is weergegeven in tabel 1:

	Informatie t.b.v. bescherming (koude fase)	Informatie t.b.v. incident response (warme fase)
Strategisch / Tactisch	**[Lessons identified]** onderlinge uitwisseling van niet-technische inzichten m.b.t. het afhandelen of voorkomen van cyberincidenten (bijv. interne en externe communicatie, organisatorische wijzingen, inhuur expertise, etc.) **[Adviesrapportages]** op basis van ontwikkelingen in cyber security (bijv. factsheets, whitepapers, implementatierichtlijnen, etc.) **[Trendanalyses]** strategische overzichten van cyber security ontwikkelingen (bijv. annual vendor reports, CSBN, global forecasts, etc.) **[Statistieken]** onderlinge uitwisseling van statistieken over cyberdreigingen (bijv. impact van incidenten, verstoringspercentages, etc.) **[Strategische actor informatie]** informatie over aanvallende actoren (bijv. profielen, wijze van optreden, capabilities, motivatie, etc.) **[Juridisch advies]** (bijvoorbeeld richtlijnen, omgang met wet- en regelgeving, *compliance* standaarden, etc.)	**[Impactanalyses]** het onderling uitwisselen van inzicht in de impact van incidenten (bijv. financiële schade, verstoring productiecontinuïteit, diefstal informatie) **[Crisiscommunicatie-advies]** Informatie ter ondersteuning van interne en externe communicatie tijdens een incident **[Juridische bijstand]** informatie ter ondersteuning van de afhandeling van een incident
Operationeel / Technisch	**[Indicators of compromise]** Technische informatie om te beoordelen of systemen getroffen zijn (bijv. malware/exploit file signatures, network traffic patterns, etc.) **[Tactieken, technieken en procedures (TTPs)]** informatie over aanvalstechnieken en werkwijze (bijv. malware analysis reports, modus operandi, etc.) [Beveiligingsinstellingen] (bijv. firewall configuraties, VPN protocollen, BYOD-instellingen). **[Operationele actor informatie]** informatie over aanvallende actoren (bijv. profielen, tactieken en technieken, user names, etc.). **[Operationele statistieken]** over impact van cyberdreigingen (bijvoorbeeld outage percentage) **[Vulnerabilities, exploits en malware]** informatie over bekende kwetsbaarheden, exploits en malware die gebruik maakt van kwetsbaarheden (bijv. CVE, shellcodes, etc.). **[Fixes en patches]** informatie over het verhelpen van kwetsbaarheden. **[Blacklists en whitelists]** Een lijst met gegevens die door middel van gegevensvergelijking bepaalt of toegang verleend of ontzegd wordt	**[Tijd-kritische informatie]** informatie bij een acute dreiging (bijv. kwetsbare systemen, infrastructuur, targets) **[Technische incident informatie]** onderlinge uitwisseling van informatie over gevonden kwetsbaarheden in de eigen organisatie **[Incident respons informatie]** informatie ter ondersteuning van (interne) operationele respons van een incident

Tabel 1) Indeling en overzicht soorten cyber cybersecurity-informatie (TNO)

Sommige deelnemers van de simulatiesessies gaven aan cybersecurity enkel op operationeel niveau te verwerken in hun organisatie . Toch kunnen deze organisaties behoefte hebben aan bepaalde soorten strategische informatie. Operationele medewerkers willen in dat geval van bepaalde strategische ontwikkelingen op de hoogte worden gehouden. Om die reden zijn sommige soorten cybersecurity-informatie zowel bij strategisch/tactisch gebruik als bij operationeel/technisch gebruik ingedeeld.

Gebruik van het overzicht en indeling soorten cybersecurity-informatie

Het overzicht van soorten cybersecurity-informatie wordt door het CWB gebruikt om informatie gericht te delen en te verzamelen met CWB-deelnemers. Het overzicht stelt het CWB en deelnemende organisaties in staat om:

- Na te gaan welke soorten cybersecurity-informatie beschikbaar zijn;
- Te evalueren welke soorten cybersecurity-informatie wordt rondgestuurd, geduid en gebruikt ;
- Op basis van de kenmerken van deelnemende organisaties te bepalen welke informatie wordt gedeeld.

Het overzicht en de indeling ondersteunen het filteren van cybersecurity-informatie door het CWB en de deelnemers. In de praktijk moet blijken in hoeverre cybersecurity-informatiedeling aan de hand van het overzicht van soorten cybersecurity-informatie in het CWB wordt gebruikt. Het CWB heeft aangegeven dat het gebruik van de indeling en het overzicht van de soorten cybersecurity-informatie enige oefening en gewenning vereist.

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

digital trust center.