TLP: AMBER

Afweegkader verdeling incidenten

Inschaling voor Raamovereenkomst IR

De Nederlandse zorg digitaal veilig

TN499559 Afweegkader verdeling incidenten - versienummer 1 - 2025

Inhoudsopgave

Inleiding

Z-CERT sluit via een aanbesteding vier (4) raamovereenkomsten af. Dit bestaat uit twee aanbieders per perceel. De volgende percelen worden daarbij onderscheiden:

- Perceel 1: Beschikbaarheidscategorie A, kan voorzien in minimaal:
  - Minimaal 10 incidenten per jaar
  - Minimaal 1 incident tegelijkertijd
  - Minimaal 1 gekwalificeerde medewerker per incident
- Perceel 2: Beschikbaarheidscategorie B, kan voorzien in minimaal:
  - Minimaal 20 incidenten per jaar
  - Minimaal 3 incidenten tegelijkertijd
  - Minimaal 3 gekwalificeerde medewerkers per incident.

Dit document gebruikt Z-CERT voor een objectieve verdeling van opdrachten binnen de aanbesteding voor Incident Response. Met dit afwegingskader besluit Z-CERT per incident of het onder perceel 1 of perceel 2 valt. Hierna wordt de procedure verder gevolgd om eerstvolgende leverancier in contact te brengen met de zorgorganisatie.

Context

Z-CERT is het expertisecentrum voor cybersecurity in de zorg. De missie van Z-CERT is de zorg digitaal veiliger maken. Dit doet Z-CERT door zorginstellingen weerbaar te maken tegen cybercriminelen. **Z-CERT** gaat binnen de **Cyberbeveiligingswet** aangewezen worden als sectoraal CSIRT en vanuit haar wettelijke taak zorgorganisaties ondersteunen bij cybersecurity-incidenten.

Omdat niet alle werkzaamheden die benodigd zijn in de afhandeling van een incident onder de wettelijke taak vallen, heeft Z-CERT besloten om de markt te betrekken en beschikbaarheid van experts te garanderen voor incident response werkzaamheden. Dit doet Z-CERT via de bovenstaande aanbesteding.

Werkproces

Onder de Cyberbeveiligingswet hebben NIS2-entiteiten te maken met een meldplicht van incidenten. De eerste melding vind plaats binnen 24 uur na ontdekking van een incident. Als sectoraal CSIRT behandeld Z-CERT deze meldingen. Dit afwegingskader valt onder het werkproces van het eerste contact bij incidenten.

Verdeling

Op basis van de criteria in het volgende hoofdstuk wordt onderscheid gemaakt tussen perceel 1 en perceel 2. In totaal zijn 6 criteria. Incidenten die aan tenminste 3 criteria voldoen, vallen onder perceel 2.

Criteria

De afweging vind plaats aan de hand van een optelsom van de onderstaande criteria. Ter verduidelijking zijn de criteria aangevuld met voorbeelden.

- Het incident heeft grote (mogelijke) gevolgen voor de zorg. Voorbeelden daarvan zijn:
    - Incidenten die leiden tot een (gedeeltelijke) opnamestop van patiënten/cliënten;
    - Incidenten die leiden tot een (gedeeltelijke) sluiting van operatiekamers en/of de spoedeisende hulp;
    - Incidenten die leiden tot een (gedeeltelijk) afzeggen van geplande zorg;
- Het incident is complex of grootschalig, zoals:
    - Verregaande toegang tot de infrastructuur die onverklaarbaar is;
    - Verschillende soorten systemen zijn geraakt;
    - Besmetting raakt meer dan 3 verschillende segmenten in een netwerk;
    - Besmetting van ongebruikelijke en gespecialiseerde systemen;
    - De omgeving bevat meerdere koppelingen tussen verschillende organisaties.
- De werkwijze van de aanvallers is complex. Voorbeelden daarvan zijn:
    - Malware waarvan de werking of impact onbekend is;
    - Aanvallers zijn voor langere periode actief in het netwerk geweest zonder dat deze logischerwijs gedetecteerd konden worden;
    - Geavanceerde (onbekende) methodieken.
- Aanval is zeer gericht. Dit wordt getypeerd door:
    - Spearphishing met onbekende werkwijze;
    - Zeer gerichte data-exfiltratie;
    - Handelingen wijzen op veel kennis van de organisatie of de sector;
- De (geraakte) omgeving is complex.
- De voor het incident benodigde incident respons capaciteit. Om het incident tijdig op te kunnen lossen zijn in ieder geval 3 gekwalificeerde medewerkers noodzakelijk.