Stekkermandaat

Een belangrijke maatregel bij cyberincidenten is het uitschakelen van de eigen systemen om erger te voorkomen. Het is van belang dat van te voren duidelijk is wie het mandaat heeft om dit uit te voeren. Dit heet het stekkermandaat.

Protocol

Het “uitschakelen van eigen systemen” is een handeling die zorgvuldig ingebed moet zijn in een breder protocol:

Het protocol is er op gericht om snel te kunnen handelen en te voorkomen dat er tijd verloren gaat door twijfelen of het wachten op toestemming. Daarom is het mandaat belegd bij de persoon die ook de handelingen kan verrichten. Andere onderdelen van het protocol zijn:

- Wat zijn de signalen en drempelwaarden om een systeem uit te schakelen?
- Welke systemen kunnen los van elkaar worden uitgeschakeld.
- Welke handelingen moeten verricht worden om het systeem werkelijk uit te schakelen. Zijn daar sleutels of wachtwoorden voor nodig?

Dilemma’s

- Is het stekkermandaat gevoelig voor misbruik?
- Is de drempelwaarde duidelijk?
- Is de persoon met het stekkermandaat vakbekwaam en bereid om het uit te voeren?
- Wat is het gevolg van het uitschakelen van een bepaald systeem?
- Welke invloed heeft uitschakelen op de forensische opsporing?

Verkennende vragen voor een crisismanager

Ga niet her-onderhandelen over het protocol maar vertrouw op de planvorming.

- Is het uitschakelen gelukt? Wie heeft dat bevestigd?
- Is duidelijk of er nog meer systemen uitgeschakeld moeten worden?
- Welke drempelwaarden moeten daarvoor bewaakt worden en wie doet dat?
- Zijn de andere systemen stabiel of is er mogelijk onderlinge afhankelijkheid?
- Wat is precies de functie van de uitgeschakelde systemen en welke impact heeft dat?
- Wat is nodig om de functionaliteit van de systemen weer terug te krijgen?
- Scenario-denken: hoe kan dit nog erger worden.
- Bestaat er een verplichting om melding te maken, wie gaat dat doen?