European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

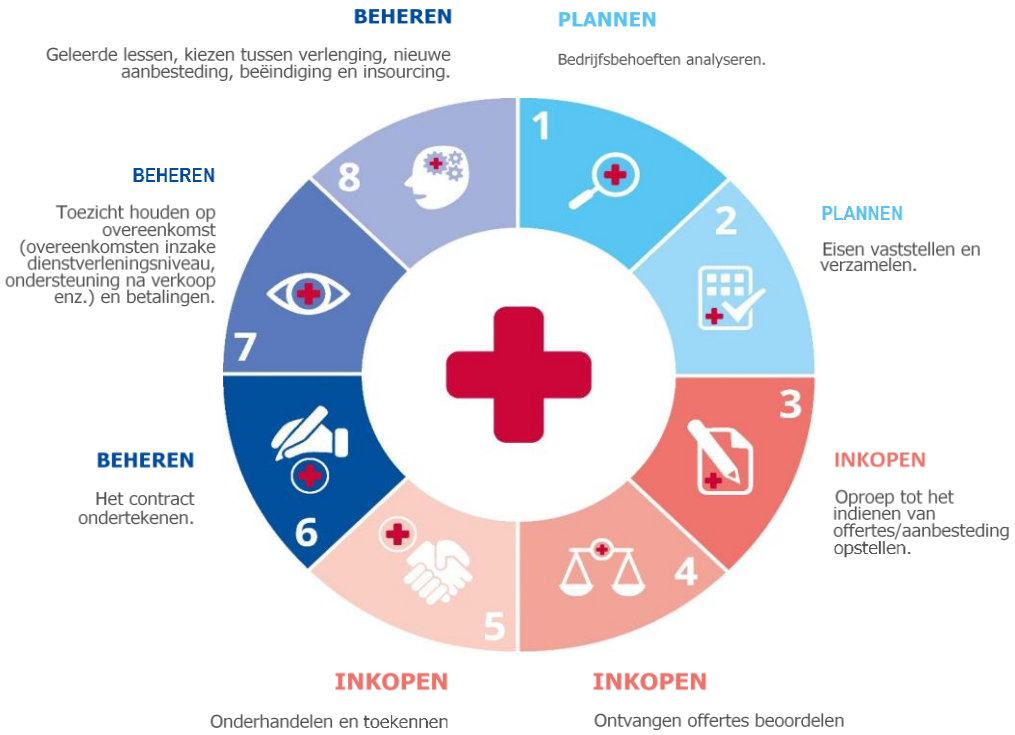
AANBESTEDINGSRICHTSNOEREN VOOR CYBERBEVEILIGING IN ZIEKENHUIZEN

Het rapport is bedoeld als “gids” voor medische beroepsbeoefenaren. Veel van de praktijken en aanbevelingen die erin worden beschreven, zullen ook nuttig zijn voor andere organisaties in de gezondheidszorg, aangezien de aanbestedingsprocedures vaak sterk op elkaar lijken. Het is nuttig voor medische beroepsbeoefenaren die technische functies in ziekenhuizen vervullen, d.w.z. op bestuursniveau: CIO, CISO, CTO, IT-teams en inkopers bij organisaties in de gezondheidszorg. In dit korte document worden de belangrijkste onderdelen van het rapport besproken. Nadere informatie is te vinden in de publicatie van ENISA: ENISA Good Practices for the Security of Healthcare Services, gepubliceerd in februari 2020.

AANBESTEDINGSPROCEDURE

Aangezien de ziekenhuisomgeving bestaat uit meerdere IT-componenten, moet de cyberbeveiliging in al deze verschillende componenten afzonderlijk worden onderzocht. Cyberbeveiliging moet deel uitmaken van alle stadia van de aanbestedingsprocedure. In dit deel presenteren we de gemeenschappelijke stadia van de aanbestedingsprocedure voor het inkopen van producten en diensten waaronder medische apparatuur, informatiesystemen en -infrastructuren.

Figuur 1: Aanbestedingsprocedurecyclus voor ziekenhuizen



- Planningsfase: In eerste instantie maakt het ziekenhuis een analyse van zijn behoeften en een interne inventarisatie van de eisen van de verschillende afdelingen. Wordt er bijvoorbeeld een nieuwe clouddienst ingekocht, dan moet de CTO onderzoeken wat de behoeften zijn en welke gebruiksmogelijkheden deze dienst biedt.

- Inkoopfase: Vervolgens worden de eisen vertaald in technische specificaties waarna, in samenwerking met de afdeling inkoop, de aanbestedingsprocedure van start gaat (er wordt bijvoorbeeld een aanbesteding gepubliceerd). Het ziekenhuis ontvangt de offertes, het comité (waarvan de CTO/CISO of iemand van het IT-team deel uitmaakt) beoordeelt de offertes en selecteert de meest geschikte producten. Er vinden onderhandelingen met de contractant plaats, waarna de overeenkomst wordt gegund.

- Beheerfase: Ten slotte wordt de overeenkomst (beheer en monitoring) overgedragen aan de opdrachtgever binnen het ziekenhuis. De aangewezen functionaris is verantwoordelijk voor de gunningsprocedure en het ontvangen van feedback van gebruikers over de werking van de apparatuur/het systeem/de dienst in de praktijk.

SOORTEN AANBESTEDINGEN IN ZIEKENHUIZEN

Tabel 1: Soorten aanbestedingen (taxonomie van bedrijfsmiddelen)

Soort aanbesteding	Beschrijving
Klinische informatiesystemen	Waaronder inkoop van ieder soort software dat dient voor medische zorg
Medische apparaten	Ieder apparaat dat bestemd is voor de behandeling, controle of diagnose van ziekten
Netwerkapparatuur	Netwerklijnen (coaxiaal, glasvezel), gateways, routers, switches, firewalls, VPN's, systemen voor detectie en preventie van inbraak enz.
Systemen voor zorgverlening op afstand	Faciliteiten of apparaten waarmee extramurale zorg wordt verleend, met name ziekenhuis- en instellingszorg thuis
Mobiele clientapparaten	Alle softwareprogramma's waarmee medische bijstand wordt verleend of waarop medische gegevens worden verzameld en die niet rechtstreeks met het netwerk van het ziekenhuis zijn verbonden, bijvoorbeeld telegeneeskundige apps
Identificatiesystemen	Systemen voor het op unieke wijze identificeren van patiënten of medisch personeel (biometrische scanners, kaartlezers enz.) en het garanderen van identificatie en/of autorisatie voor toegang tot de IT-systemen
Gebouwbeheersystemen	Ieder type bouwwerk dat medische faciliteiten kan bevatten
Industriële regelsystemen	Systemen waarmee alle fysieke aspecten van de instellingen worden geregeld, zoals energievoorziening, deurvergrendeling, bewakingscamera's
Professionele diensten	Alle soorten al dan niet uitbestede diensten die worden verleend door professionals of bedrijven: medische diensten, vervoer, boekhouding, machinebouw, IT, juridisch, onderhoud, reiniging, catering enz.
Clouddiensten	Ieder computer- of ander informatiesysteem dat zich niet bevindt in de medische instelling of een datacentrumfaciliteit waarover de IT-afdeling van de medische instelling volledige zeggenschap heeft

TAXONOMIE VAN DREIGINGEN

Bij de verschillende soorten dreigingen voor de ICT-omgeving van een ziekenhuis horen verschillende soorten aanbestedingen. Raadpleeg de taxonomie van dreigingen in dit deel samen met uw afdeling IT, Beveiliging of Risicobeheer om te bepalen met welke dreigingen uw organisatie het meest te maken heeft. Deze activiteit moet deel uitmaken van de IT-taken in het ziekenhuis ongeacht het aanbestedingspotentieel.

Tabel 2: Soorten dreigingen (taxonomie van dreigingen)

Dreiging	Voorbeelden
Natuurverschijnselen	Brand, overstroming, aardbeving
Storing in de toeleveringsketen	Storing bij de cloudaanbieder, storing bij de netwerkaanbieder, elektriciteitsstoring, storing bij fabrikant van medische apparatuur / niet-aansprakelijkheid
Menselijke fouten	Configuratiefout in medisch systeem, ontbreken van audit trail, ontbreken van of fout in controle op ongeoorloofde toegang, niet-naleving (BYOD), fout door medisch personeel / patiënt
Kwaadaardige handelingen	Malware (virus, gijzelsoftware, BYOD), kaping (cryptojacking, medjacking), social engineering (phishing, baiting, device cloning), diefstal (gegevens, apparaat), vervalsing van medische apparatuur, skimmen, Denial of Service, aanvallen via het web, webapplicatieaanvallen, dreiging van binnenuit, fysieke manipulatie / beschadiging, identiteitsdiefstal, cyberspionage, mechanische ontregeling van componenten
Systeemstoringen	Softwarefout, verouderde firmware, apparaatstoring, storing in netwerkcomponenten, ontoereikend onderhoud

GOEDE PRAKTIJKEN VOOR CYBERBEVEILIGING BIJ AANBESTEDINGEN

De onderstaande lijst van goede praktijken is allerminst volledig, maar biedt de IT-functionaris in de gezondheidszorg die verantwoordelijk is voor de inkoop van ziekenhuisapparatuur een gedegen handvat. De lijst van goede praktijken is het gecombineerde resultaat van alle input die is ontvangen van functionarissen in de gezondheidszorg met wie vraaggesprekken zijn gehouden. De lezer kan de lijst aanpassen aan de hand van de prioriteiten van zijn/haar organisatie.

GP 1. Betrek de IT-afdeling bij de verschillende stadia van de aanbesteding om ervoor te zorgen dat de nodige deskundigheid met betrekking tot cyberbeveiligingsaspecten in aanmerking wordt genomen.

Aanbestedingsfasen: Alle

Betrokken soorten aanbestedingen: Alle

Betrokken dreigingen: Alle

GP 2. Pas een procedure toe voor de identificatie en het beheer van kwetsbaarheden zodat kwetsbaarheden in aanmerking worden genomen vóór de aanbesteding van nieuwe producten of diensten en zodat de kwetsbaarheden van bestaande producten/diensten gedurende de gehele levenscyclus ervan worden gemonitord.

Aanbestedingsfasen: Alle

Betrokken soorten aanbestedingen: Klinische informatiesystemen, medische apparaten, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Alle

GP 3. Stel een beleid op voor hardware- en software-updates om ervoor te zorgen dat de meest recente patches voor uw besturingssysteem en software worden geïnstalleerd en dat de antivirussoftware wordt bijgewerkt.

Aanbestedingsfasen: Alle

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 4. Versterk de veiligheidscontroles voor draadloze communicatie om ervoor te zorgen dat de toegang tot de Wireless LAN-netwerken van het ziekenhuis beperkt is en streng wordt gecontroleerd.

Aanbestedingsfasen: Alle

Betrokken soorten aanbestedingen: Medische apparaten, client-op-afstandapparaten, identificatiesystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, menselijke fouten

GP 5. Stel een testbeleid vast om ervoor te zorgen dat nieuw aangeschafte of nieuw geconfigureerde producten een penetratietest ondergaan en dat de beschermingsmaatregelen worden toegesneden op de operationele parameters van de feitelijke omgeving.

Aanbestedingsfasen: Alle

Betrokken soorten aanbestedingen: Klinische informatiesystemen, medische apparaten, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, gebouwbeheersysteem, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, systeemstoringen, menselijke fouten

GP 6. Stel bedrijfscontinuïteitsplannen vast om ervoor te zorgen dat de kerndiensten van het ziekenhuis niet door een systeemstoring worden ontregeld en dat de rol van de leverancier goed is omschreven.

Aanbestedingsfasen: Alle

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 7. Houd rekening met interoperabiliteit om ervoor te zorgen dat er geen beveiligingslacunes zijn tussen nieuwe en reeds bestaande componenten (legacy-IT).

Aanbestedingsfasen: Alle

Betrokken soorten aanbestedingen: Klinische informatiesystemen, medische apparaten, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Systeemstoringen, menselijke fouten, kwaadaardige handelingen

GP 8. Zorg ervoor dat alle componenten kunnen worden getest zodat u er zeker van bent dat ze werken zoals toegezegd: controleer of de oplossing gemakkelijk te gebruiken is, of de resultaten onder belasting juist zijn en of de beveiliging zwakke plekken (zwak wachtwoordbeleid, SQL-injectie) vertoont.

Aanbestedingsfasen: Alle

Betrokken soorten aanbestedingen: Klinische informatiesystemen, medische apparaten, clientapparaten op afstand, identificatiesystemen, clouddiensten, industriële regelsystemen, telezorgsysteem, gebouwbeheersysteem, mobiele clientapparaten

Betrokken dreigingen: Kwaadaardige handelingen, menselijke fouten, systeemstoringen, storing in toeleveringsketen

GP 9. Zorg voor auditing en logging om aanvallers te kunnen traceren en om te kunnen vaststellen hoeveel informatie verloren is gegaan/gestolen bij een defect of beveiligingslek in het systeem.

Aanbestedingsfasen: Alle

Betrokken soorten aanbestedingen: Medische apparaten, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 10. Versleutel gevoelige persoonsgegevens bij opslag en doorvoer door een beleid te definiëren voor systemen, diensten of apparaten waarmee bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9 van de AVG worden verwerkt.

Aanbestedingsfasen: Alle

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 11. Voer een risicobeoordeling uit als onderdeel van de aanbestedingsprocedure.

Aanbestedingsfasen: Plannen

Betrokken soorten aanbestedingen: Alle

Betrokken dreigingen: Alle

GP 12. Plan de eisen aan het netwerk, de hardware en de licenties van tevoren om vast te stellen of er voorafgaand aan de installatie aanvullende upgrades en/of aankopen moeten worden verricht ten behoeve van het nieuwe systeem.

Aanbestedingsfasen: Plannen

Betrokken soorten aanbestedingen: Klinische informatiesystemen, netwerkapparatuur, identificatiesystemen, industriële regelsystemen.

Betrokken dreigingen: Storing in toeleveringsketen, systeemstoringen, natuurverschijnselen, menselijke fouten

GP 13. Breng dreigingen in verband met aanbestedingen van producten of diensten in kaart en zorg ervoor dat gedurende de hele levenscyclus van ingekochte producten/diensten dreigingen worden geïdentificeerd.

Aanbestedingsfasen: Plannen, beheren

Betrokken soorten aanbestedingen: Alle

Betrokken dreigingen: Alle

GP 14. Zorg voor een scheiding van netwerkonderdelen om ervoor te zorgen dat netwerkverkeer kan worden geïsoleerd en/of gefilterd zodat toegang van de ene netwerkzone naar andere kan worden beperkt en/of geblokkeerd.

Aanbestedingsfasen: Plannen, inkopen

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 15. Bepaal welke eisen aan het netwerk worden gesteld om te zorgen voor interoperabiliteit en om hiaten te voorkomen nadat de topologie van het netwerk en de componenten is gecreëerd.

Aanbestedingsfasen: Plannen

Betrokken soorten aanbestedingen: Klinische informatiesystemen, netwerkapparatuur, identificatiesystemen, industriële regelsystemen, clouddiensten, telezorgsystemen, mobiele clientapparaten.

Betrokken dreigingen: Storing in toeleveringsketen, systeemstoringen, natuurverschijnselen

GP 16. Stel basiseisen aan de beveiliging vast en vertaal deze naar toelatingscriteria bij het kiezen van leveranciers.

Aanbestedingsfasen: Plannen, inkopen

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 17. Breng een afzonderlijke oproep tot het indienen van offertes uit voor de aanbesteding van clouddiensten en houd daarbij rekening met de wettelijke eisen en de eisen op grond van uw beleid.

Aanbestedingsfasen: Plannen, inkopen

Betrokken soorten aanbestedingen: Clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen

GP 18. Koop bij voorkeur bedrijfsmiddelen in die zijn gecertificeerd op grond van stelsels/normen inzake cyberbeveiliging.

Aanbestedingsfasen: Inkopen

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 19. Voer bij het plannen van de aanbesteding van een nieuw systeem of nieuwe dienst gegevensbeschermingseffectbeoordelingen uit.

Aanbestedingsfasen: Inkopen

Betrokken soorten aanbestedingen: Klinische informatiesystemen, medische apparaten, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, professionele diensten, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, menselijke fouten

GP 20. Richt de gateways zo in dat legacysystemen/-apparaten verbonden blijven en dat afscherming mogelijk is voor het geval zich binnen deze groepen problemen voordoen.

Aanbestedingsfasen: Inkopen, beheren

Betrokken soorten aanbestedingen: Medische apparaten, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 21. Zorg voor training om ervoor te zorgen dat interne personeelsleden, evenals externe contractanten/adviseurs die op locatie komen werken, voldoende vertrouwd zijn met de cyberbeveiligingspraktijken van de organisatie.

Aanbestedingsfasen: Inkopen, beheren

Betrokken soorten aanbestedingen: Alle

Betrokken dreigingen: Kwaadaardige handelingen, menselijke fouten

GP 22. Stel plannen voor respons bij incidenten op voor nieuw ingekochte producten of systemen.

Aanbestedingsfasen: Inkopen, beheren

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 23. Betrek de leverancier/fabrikant bij het incidentenbeheer en stel in de oproep tot het indienen van offertes duidelijke voorwaarden vast.

Aanbestedingsfasen: Inkopen, beheren

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 24. Plan en monitor onderhoudswerkzaamheden voor alle apparatuur om een adequate werking te garanderen en bepaal een keuze voor updates/patches enz.

Aanbestedingsfasen: Inkopen, beheren

Betrokken soorten aanbestedingen: Klinische informatiesystemen, netwerkapparatuur, medische apparaten, gebouwbeheersystemen, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Menselijke fout, systeemstoring, natuurverschijnselen

GP 25. Toegang op afstand moet tot een minimum worden beperkt en zodanig worden beheerd dat de leverancier extern alleen kan communiceren met de apparatuur die onder zijn toezicht staat.

Aanbestedingsfasen: Inkopen, beheren

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen, menselijke fouten

GP 26. Eis dat op patches ter beschikking worden gesteld voor alle componenten en vermeld dit in de oproep tot het indienen van offertes.

Aanbestedingsfasen: Inkopen, beheren

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen

GP 27. Maak de medewerkers bewust van cyberbeveiliging zodat zij op de hoogte zijn van de risico's die verbonden zijn aan nieuw ingekochte producten of diensten.

Aanbestedingsfasen: Beheren

Betrokken soorten aanbestedingen: Alle

Betrokken dreigingen: Alle

GP 28. Inventariseer de bedrijfsmiddelen en beheer de configuratie zodanig dat de inventaris naar behoren wordt geüpdatet wanneer een component aan de ICT-omgeving wordt toegevoegd of eruit wordt verwijderd, en dat basisbeveiligingsconfiguraties voor de ICT-componenten zijn ingesteld en op passende wijze worden beheerd.

Aanbestedingsfasen: Beheren

Betrokken soorten aanbestedingen: Klinische informatiesystemen, medische apparaten, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen

Betrokken dreigingen: Kwaadaardige handelingen, menselijke fouten, systeemstoringen

GP 29. Stel speciale toegangscontrolemechanismen vast voor faciliteiten met medische apparatuur die ook fysiek moeten worden beveiligd en uitsluitend toegankelijk zijn voor gespecialiseerd personeel.

Aanbestedingsfasen: Beheren

Betrokken soorten aanbestedingen: Medische apparaten, gebouwbeheersysteem, identificatiesystemen

Betrokken dreigingen: Kwaadaardige handelingen, menselijke fouten

GP 30. Zorg voor penetratietests op gezette tijden of na een wijziging in de architectuur/het systeem en neem desbetreffende voorwaarden op in de oproep tot het indienen van offertes.

Aanbestedingsfasen: Inkopen, beheren

Betrokken soorten aanbestedingen: Medische apparaten, klinische informatiesystemen, netwerkapparatuur, telezorgsysteem, mobiele clientapparaten, identificatiesystemen, industriële regelsystemen, clouddiensten

Betrokken dreigingen: Kwaadaardige handelingen, storing in toeleveringsketen, systeemstoringen