Checklist Digitale Weerbaarheid

Inleiding

Het Traumacentrum-ZWN is samen met de GHOR-bureaus Zeeland, Zuid-Holland Zuid en Rotterdam-Rijnmond het project 'Digitale Weerbaarheid' gestart met het doel om eind 2022 in de hele regio beter voorbereid te zijn en het bewustzijn te vergroten op het gebied van digitale weerbaarheid. Trimension ondersteunt het project. Na het uitvoeren van de nulmeting in de regio, die de stand van zaken op het gebied van digitale weerbaarheid bij instellingen in de regio heeft blootgelegd, is de Crisis Toolbox 'Digitale weerbaarheid in de zorg' gemaakt. Hierin zijn verschillende tools te vinden die de instellingen helpen om digitale weerbaarheid te verhogen, zoals deze checklist, maar ook een handleiding voor een interne Crisistafel en een handleiding voor een interne oefening. De Crisis Toolbox is vrij toegankelijk voor elke zorginstelling in de regio en tussentijds aangevuld.

Digitale weerbaarheid

Digitale weerbaarheid is *"het vermogen om relevante risico's van digitale incidenten tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om incidenten te voorkomen, snel te ontdekken, schade te beperken en herstel eenvoudiger te maken."* Voor de nulmeting zijn hier zeven indicatoren uit gekomen die samen digitale weerbaarheid vormen.

Toelichting

In dit document vind je een checklist voor digitale weerbaarheid in jouw organisatie. In deze checklist vind je handelingen die jouw organisatie verder helpen om digitaal weerbaarder te worden. De checklist is ingedeeld aan de hand van de zeven indicatoren van digitale weerbaarheid. Per indicator is een aantal stappen aangegeven die jouw organisatie kan uitvoeren om weerbaarder te worden. Daarnaast bestaan al veel nuttige hulpmiddelen op het gebied van digitale weerbaarheid die zijn ontwikkeld door andere organisaties. Deze worden in dit document gelinkt en zijn zeer goed bruikbaar.

Doelstelling en doelgroep

Het doel van deze checklist is om een handvat te bieden waar je als organisatie aan kunt denken, of welke stappen je kunt ondernemen om de digitale weerbaarheid te verhogen. Deze checklist is bedoeld voor OTO-functionarissen, crisiscoördinatoren en/ of functionarissen op het gebied van IT en Cybersecurity, zoals een Chief Information Security Officer.

Checklist

Risicomanagement

"De kans dat een incident op het gebied van digitale weerbaarheid zich voordoet en de impact daarvan, beide in relatie tot het niveau van de actuele weerbaarheid."

- Maak inzichtelijk welke processen binnen de organisatie afhankelijk zijn van IT zodat duidelijk is op welke processen een digitale verstoring de meeste impact heeft.
- Voer een security risk assessment uit om de IT-risico's en cyberdreigingen die van toepassing zijn op jouw organisatie in kaart te brengen.
- Breng afhankelijkheden op het gebied van digitale weerbaarheid met externen, zoals ketenpartners en leveranciers, in kaart om risico's op dat gebied te duiden.

Ondersteunend materiaal

- Het Z-CERT stelt jaarlijks het Cybersecurity Dreigingsbeeld Zorg op. Hierin staat veel beschreven over risico's, dreigingen, incidenten. Hier staan ook tips en tricks beschreven.
- In de Infographic Telekwetsbaarheid staat in vijf stappen beschreven hoe je je als organisatie kunt voorbereiden op uitval van telecom en IT.

Beveiligingsbewustzijn

"De mate waarin mensen risico's van digitale incidenten herkennen en zich ervan bewust zijn dat deze de veiligheid van informatie in gevaar kunnen brengen."

- Maak een handleiding voor de incidentmeldingsprocedure en maak deze breed bekend in de organisatie, zodat alle medewerkers weten hoe ze een incident moeten melden.
- Train medewerkers elk half jaar in beveiligingsbewustzijn, zodat hun kennis up-to-date blijft en steeds wordt aangevuld met nieuwe ontwikkelingen en nieuwe risico's.
- Maak overzichtelijke hand-outs met de belangrijkste punten voor beveiligings-bewustzijn en plaats deze fysiek op verschillende opvallende plekken in de organisatie zodat medewerkers de informatie over beveiligingsbewustzijn continue zien en er bekend mee raken.

Ondersteunend materiaal

- Op www.informatieveiliggedragzorg.nl vind je een platform om informatieveilig gedrag in jouw organisatie te stimuleren.
- Het Z-CERT heeft een document gemaakt dat in je organisatie opgehangen kan worden en informatie geeft over hoe medewerkers van jouw organisatie veilig thuis en op kantoor kunnen werken. De hand-out vind je hier: Cyber Fit.

Opleiden, Trainen, Oefenen (OTO)

"1) Het bijbrengen van kennis en vaardigheden in opleidingen, 2) het opdoen van praktijkervaring met bepaalde vaardigheden in trainingen en 3) het simuleren van een situatie en mensen laten handelen binnen dit kader in oefeningen."

- Integreer het onderwerp digitale weerbaarheid in het nieuwe OTO-plan, zodat het onderwerp een terugkerende factor is.
- Test regelmatig procedures over hoe om te gaan met een digitaal incident door middel van een oefening om continue scherp te houden of de procedures nog voldoende zijn.
- Oefen digitale incidenten regelmatig met ketenpartners.
- Verzorg een training met bestuurders op het gebied van digitale weerbaarheid om hun bewustzijn en vaardigheden op dit gebied te verhogen en draagvlak voor dit onderwerp binnen de eigen organisatie te stimuleren.

Ondersteunend materiaal

- In de Crisis Toolbox 'Digitale weerbaarheid' (gemaakt vanuit dit project) vind je een handleiding om een interne Crisistafel rondom verschillende type digitale verstoringen te organiseren (cyber en IT-uitval). Het doel van deze (laagdrempelige) werkvorm, die je zelf kan organiseren, is om de onderlinge samenwerking, verwachtingen en afhankelijkheden tussen verschillende betrokkenen en systemen tijdens een digitale verstoring concreet inzichtelijk maken. Daarmee krijg je als organisatie zicht op eventuele kwetsbaarheden en kan je gerichter werken aan je digitale weerbaarheid.
- In de Crisis Toolbox 'Digitale weerbaarheid' komt na de zomer (2022) ook een handleiding aan de hand waarvan je intern een crisisoefening op het gebied van digitale weerbaarheid kan organiseren.

Crisismanagement

"Acties en maatregelen om een crisis in een organisatie te voorkomen of op te lossen. Een crisis is een noodsituatie waarbij de continuïteit van een organisatie ernstig verstoord raakt."

- Maak een (papieren) lijst met werkafspraken bij noodsituaties, zodat je deze tijdens een crisis erbij kunt pakken. Denk bijvoorbeeld aan het continueren van processen op een andere manier dan regulier.
- Neem digitale weerbaarheid op in de crisisplanvorming, bijvoorbeeld in de vorm van een scenariokaart.
- Neem digitale weerbaarheid op in een bedrijfscontinuïteitsplan, zodat je tijdens een incident al inzichtelijk hebt hoe bepaalde processen voort te zetten.

Ondersteunend materiaal

- Het Nationaal Crisisplan Digitaal helpt de vertaalslag te maken van de crisisaanpak op nationaal niveau naar operationeel uitgewerkte plannen en draaiboeken voor overheden en sectoren zoals de zorg.
- Het Z-CERT heeft een stappenplan Eerste Hulp Bij Datalekken (EHBD) gemaakt voor de zorgsector dat weergeeft wat te doen als jouw organisatie is betrokken bij een datalek.

Dagelijkse Organisatie

"De manier waarop taken, processen en procedures die voorwaardelijk zijn voor het verhogen van digitale weerbaarheid zijn georganiseerd in de organisatie."

- Bewaar oude werkwijzen, zodat je daarop kunt terugvallen wanneer er een digitale verstoring is.
- Implementeer een duidelijk beveiligingsbeleid en zorg dat dit breed binnen de organisatie bekend is.
- Zorg voor een incidentlog systeem, zodat incidenten goed gemonitord kunnen worden en je later kunt terugvallen op de logs voor onderzoek of evaluatie.
- Zorg voor rolhouders binnen de organisatie die zich actief bezig houden met digitale weerbaarheid, zoals een Chief Information Security Officer (CISO) of een Information Manager.

Ondersteunend materiaal

- Het Z-CERT heeft een tool gemaakt om inzicht te krijgen in hoe jouw organisatie ervoor staat ten aanzien van de NEN 7510[1] en de AVG[2].
- De Cybersecurity Raad heeft een Handreiking Cybersecurity voor de Bestuurder gemaakt die inzicht geeft in hoe bestuurders cybersecurity kunnen beleggen binnen de organisatie.

Netwerk

"De mate van aandacht die wordt besteed aan afhankelijkheden van en het veilig samenwerken met partners in het netwerk."

- Praat met partners in je netwerk over het niveau van digitale weerbaarheid bij hen en bespreek wat jullie van elkaar verwachten op dit gebied. Denk bijvoorbeeld aan een bepaalde manier van informatieoverdracht.
- Breng in kaart met welke partners samengewerkt kan worden op het gebied van digitale weerbaarheid.
- Maak een overzicht van leveranciers van hard- en software en welke leveranciers op afstand een dienst verlenen zodat het inzichtelijk is waar afhankelijkheden liggen.

Ondersteunend materiaal

- De Handreiking Ketencommunicatie bij Crises van het Centrum Informatiebeveiliging en Privacybescherming (CIP) biedt een generieke opzet voor een ketencrisiscommunicatieprotocol. Je kunt de handreiking invullen en aanvullen met proces-eigen kenmerken. Zo ontstaat een communicatieprotocol, dat kan worden gebruikt voor de communicatie met keten/netwerkpartners en overige stakeholders.
- Wees daarnaast alert op netwerk/ketenoefeningen die vanuit de (veiligheids/GHOR)regio worden georganiseerd op dit thema. Maar ook met een delegatie kleinschalig scenario('s) doorlopen met andere instellingen uit de regio is al heel waardevol.

Ambitie voor digitale weerbaarheid

"Wat een organisatie wil bereiken op het gebied van digitale weerbaarheid."

- Formuleer een heldere visie voor digitale weerbaarheid zodat het duidelijk is wat jouw organisatie verstaat onder digitale weerbaarheid en wat dit betekent voor jouw organisatie.
- Formuleer zowel een korte en een lange termijn ambitie voor digitale weerbaarheid zodat jouw organisatie een stip op de horizon heeft om naartoe te werken.
- Maak een stappenplan om naar de ambitie toe te werken.

[1] De norm NEN 7510 (afgeleide van ISO 27001) is toegesneden op informatiebeveiliging binnen de gezondheidszorg. Hieronder wordt verstaan het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie ten behoeve van verantwoorde zorg voor patiënten.
[2] De Algemene Verordening Gegevensbescherming (AVG) is de Europese privacywetgeving, die sinds 25 mei 2018 in de hele Europese Unie (EU) geldt. De AVG gaat over de bescherming van persoonsgegevens.