Bijlage bij het verslag van het vierde Regionaal Kennisplatform Integraal Crisisplan Zorg: concept scenariokaart Cyberaanval (mei 2016)

In deze scenariokaart staan bijzonderheden/aandachtspunten in aanvulling op de generieke integrale crisisaanpak zoals beschreven in de notitie *Bouwstenen Integraal Crisisplan.* Dit is een illustratie van hoe een scenariokaart kan worden ingevuld. Dit conform bijlage 3 van de bouwstenen.

Type crisis	Cybercrisis : Een abnormale en onstabiele situatie waarbij strategische doelen, reputatie en betrouwbaarheid in het geding komen doordat een verstoring van de IT, bewust of onbewust, het hart van de organisatie raakt.
Bijzonderheden crisisprofiel?	
Belangrijkste impactgebieden en bijzonderheden qua impact?	Juridische aspecten, zorg continuïteit (afhankelijk van geraakte systemen), IT/ bedrijfscontinuiteit, privacy, interne communicatie, externe communicatie, bedrijfscontinuïteit /logistiek, opsporing. Er is altijd een onderzoekscomponent (wat is er aan de hand? Waar zitten effecten?). Als personeelsgegevens betrokken zijn is er ook een HR component. Het kan gaan om een storing, een onbedoeld/bedoeld beschikbaar/toegankelijk zijn van data of een moedwillige aanval en/of chantage
Specifieke doelstellingen en uitgangspunten?	Doelstellingen: • Bedrijfscontinuïteit waarborgen • Voorkomen van gevolgen voor de patiëntveiligheid • Beperken van onrust onder patiënten, medewerkers en derden • Behouden en/of herstellen van vertrouwen in de instelling Uitgangspunten: • Veiligheid van personeel, patiënten en bezoekers staat voorop • Wij schakelen zo snel mogelijk externe expertise in (voorbeeld is Z-cert) • We informeren de medewerkers op basis van *'need to know'* • We werken op basis van feiten (informatiegestuurd i.p.v. risicogestuurd) en proberen deze zo snel mogelijk in kaart te brengen • We blijven niet werken met of in een onbetrouwbaar systeem en accepteren de financiële gevolgen in dit kader • Instanties zoals de AP(= Autoriteit Persoonsgegevens) worden op de hoogte gebracht bij een Datalek • We gaan nooit in op chantage • In het uiterste geval gaan kwaliteit en veiligheid voor privacy
Mogelijke kritieke momenten en besluiten?	Kritieke momenten: • Vaststelling van de Cyberincident • Vaststelling van het moment dat sprake is van een crisis • Vaststelling van geweken gevaar Kritieke besluiten : • Het moment dat wordt overgegaan op Noodprocedures • Het al dan niet stopzetten van vitale systemen/processen • Het besluiten tot een (tijdelijke)patiëntenstop • Het besluit dat er niet langer meer sprake is van verantwoorde zaken • Bevriezen / terugzetten gegevens (communiceren richting systeemeigenaren en afdelingshoofden): actuele data in het geding en nadien veel re-work. • Het moment en de wijze van externe communiceren
Bijzondere stakeholders/netwerk-partners?	Interne partners: • Juridisch adviseur • Privacy Officer • Security Officer • RvB • RvT • ICT • Communicatie • Facilitair bedrijf

	Externe Partners: • Z-cert (vergt een contract vooraf, mogelijk wel benaderbaar voor advies), breder: nationaal cyber security center (NCSC) • Politie • Gemeente Stakeholders: Autoriteit Persoonsgegevens, IGZ Zorgketenpartners: • Meldkamer ambulance, ziekenhuizen, huisartsen, Lab, etc. • Ziektekostenverzekeraars
Bijzonderheden in de voorbereiding?	
Specifieke voorzieningen voorbereid?	• IT-respons team? • Samenwerking/afstemming met Z-Cert (= Computer Emergency Response Team Zorgsector) • Mogelijkheid inzet extra IT capaciteit (extern) • Aansluiting IT op crisismanagementstructuur
Aanvullende benodigde externe expertise	• Mogelijk noodzaak van aanvullende (cyber) security kennis • Specifieke juridische expertise
Bepaalde plannen en procedures die het team niet moet vergeten?	• Calamiteiten procedures ICT, Continuïteitsplannen Zorg • Zicht op kritische patiëntengroepen / zorgprocessen
Bijzonderheden qua signaleren, alarmeren en/of informeren?	
Afwijkingen?	• Alarmeren Externe Partijen(Z-cert,AP) Interne crisis organisatie, • In gang zetten Crisismanagement • Rekening houden met mogelijkheid dat medewerkers en/of patiënten zelf ook merken dat er een verstoring is. Vergt snelle communicatie met eerste handelingsperspectief • Mogelijke kwetsbaarheid in communicatie als systemen zijn aangetast of moeten worden uitgezet
Bijzonderheden in reageren en beperken negatieve gevolgen?	
Bijzonderheden in de eerste respons?	• Begint bij detectie • Maatregelen gericht op ‘insluiten’ / verdere toegang/verspreiding voorkomen
Specifieke invulling crisisorganisatie?	• Combinatie van IT-team, crisisbeleidsteam en aansluiten facilitair en anderen. Mogelijk 2 OT’s: 1 voor bron (IT) en 1 voor effecten. Afhankelijk van impact kan dat ook in 1 OT. Privacy-officier aansluiten in CBT
Bijzonderheden in de opschaling?	• Aandachtspunt is aansluiting van de zorg
Onze rol in de keten?	• Mogelijk zijn ook andere zorginstelling slachtoffer: vergt vertrouwelijk informeren/waarschuwen bij vermoeden van opzet
Waarschijnlijke overheidsopschaling? Bijzondere overheidspartners?	• Meldplicht AP • Mogelijke aangifte bij politie
Bijzonderheden nafase en herstel?	
Bijzondere aspecten van herstel? Bv. vanwege complexiteit of lange duur?	• Controle van opnieuw opgestarte systemen / mogelijk verloren informatie • Belangrijk na herstel van de crisissituatie is het evaluatiemoment: zowel de techniek als wel het proces moet geëvalueerd worden. • Bij een cyberaanval is het belangrijk om uit te sluiten dat de dreiging tot een minimum gebracht is, hierbij is het belangrijk om aan te geven wat het dreigingsniveau is aangezien het altijd heel lastig is te bepalen of dreiging “uit het systeem is”. Vergt extra monitoring
Specifieke topics die bijzondere aandacht behoeven?	• Interne en externe terugkoppeling met evaluatieverslag • Eventuele aanpassingen in procedures • Eventuele juridische/aansprakelijkheidsissues • Goede communicatie naar patiënten en medewerkers, mogelijk heel gericht informeren wiens/welke informatie is gelekt/gestolen
Specifieke invulling nafase-organisatie?	• Herstelprocedures + formele vaststelling dat geen sprake meer is van crisis + evt onderhanden zijnde restrisico’s.