Aandachtskaart cyberdreiging

Wat is het risico?

Bij zorginstellingen zijn veel kritische zorgprocessen en systemen afhankelijk van een goede digitale beveiliging. Denk hierbij aan patiëntendossiers, medicatiebeheer en medische apparatuur die verbonden zijn met het netwerk. Een cyberdreiging, zoals een hack of ransomware-aanval, kan leiden tot ernstige verstoringen in deze processen. Daarnaast kunnen gegevens van patiënten en medewerkers blootgesteld worden, wat juridische en financiële gevolgen kan hebben. Het is voor een organisatie van groot belang om te weten welke systemen en processen kwetsbaar zijn voor cyberdreigingen. Hoe afhankelijk zijn deze processen van digitale systemen en hoe gevoelig zijn deze systemen voor aanvallen? Door risico's in kaart te brengen en een prioritering aan te brengen, kan inzicht worden verkregen in de urgentie van beveiligingsmaatregelen en alternatieve oplossingen.

Aandachtspunten bij de voorbereiding

- Als zorginstelling ben je zelf verantwoordelijk voor de eigen cyberveiligheid, waakzaamheid en weerbaarheid.
- Breng in kaart welke kritische processen en systemen afhankelijk zijn van digitale middelen. Analyseer de impact van een verstoring door cyberdreigingen en bepaal welke processen prioriteit hebben bij herstel.
- Test de digitale weerbaarheid van jouw organisatie door simulaties, zoals phishingtests of een netwerkuitval. Breng in kaart waar medewerkers en de organisatie tijdens deze tests tegenaan lopen.
- Maak afspraken met IT-dienstverleners en cybersecurity-experts over ondersteuning bij cyberincidenten. Neem 24/7 contactgegevens van deze partijen op in de plannen en procedures.
- Zorg dat plannen en procedures zowel digitaal als op papier beschikbaar zijn en regelmatig worden bijgewerkt.

Actualiseer de gegevens van jouw zorginstelling regelmatig in GHOR4all. Via deze gegevens neemt de GHOR contact op wanneer er sprake is van een cyberdreiging.

Aandachtspunten bij een (dreigende) uitval

- De daadwerkelijke uitvoering van de geneeskundige hulpverlening is en blijft steeds een verantwoordelijkheid van de zorginstellingen en zorgverleners zelf. Met andere woorden: de zorg moet ook tijdens ramp- of crisisomstandigheden verantwoord geleverd worden.
- Breng in kaart welke systemen en processen zijn getroffen.
- Analyseer welke zorgprocessen in gevaar komen en bepaal prioriteiten voor herstel.
- Voer de procedures uit zoals vastgelegd in de planvorming.

Risico's in de regio

Meer lezen over dit risicotype of andere risico's in de regio? Bekijk hier het Zorgrisicoprofiel Brabant-Zuidoost.

Wat kan je met de GHOR bespreken?

- Welke maatregelen jouw organisatie heeft getroffen om de gevolgen van een cyberdreiging of cyberincident te beperken.
- Welke knelpunten er zijn met betrekking tot de zorgcontinuïteit van jouw zorginstelling.
- Welke ondersteuning van de GHOR nodig is.

Hulp nodig bij de aandachtspunten?

Neem contact op met onze relatiebeheerders.
Zij denken graag met je mee!
infoghor@vrbzo.nl

Contact met de GHOR

- Bij (verwachte) knelpunten in de zorgcontinuïteit binnen jouw instelling kan je zelf 24/7 contact opnemen met de GHOR.
- Bel naar de Meldkamer Ambulancezorg via telefoonnummer **088 061 80 02** en vraag naar de Algemeen Commandant Geneeskundige Zorg (ACGZ) van de GHOR in jouw regio

Scenario's

Bij een cyberdreiging kunnen twee scenario's worden onderscheiden.

1. Onverwachte aanval:
   - Er is sprake van een plotselinge cyberaanval, zoals ransomware of een datalek, zonder waarschuwing vooraf.
   - IT-specialisten of cybersecurity-experts dienen de aard en impact van de aanval zo snel mogelijk te analyseren en maatregelen te nemen.

2. Voorspelde dreiging:
   - Er is sprake van een voorziene cyberdreiging, bijvoorbeeld door een waarschuwing van het Nationaal Cyber Security Centrum (NCSC) of een ontvangen dreigement.
   - Er kan preventief gehandeld worden om de schade te beperken, zoals door netwerken af te sluiten of back-ups veilig te stellen.

Handige informatie

- Z-CERT (Computer Emergency Response Team voor de zorg)
  - De cybersecurityorganisatie voor zorginstellingen. Biedt hulp bij incidenten, deelt dreigingsinformatie en geeft advies om cyberveiligheid in de zorg te verbeteren.
- NCSC (Nationaal Cyber Security Centrum)
  - Helpt bij het beschermen van vitale infrastructuur in Nederland tegen cyberdreigingen. Z-CERT en het NCSC werken nauw samen.
- NIS2 (Netwerk- en Informatiebeveiligingsrichtlijn 2)
  - Europese wetgeving die strengere cybersecurity-eisen oplegt aan essentiële en belangrijke sectoren, waaronder de zorg. Zorginstellingen moeten hierdoor hun beveiligingsmaatregelen versterken en meldplicht naleven.

Tijd	Maatregelen
0 tot 2 uur	
• Onmiddellijk verlies van toegang tot digitale systemen. • Communicatie via e-mail en interne systemen werkt niet. .	• Schakel direct de IT-dienstverlener of cybersecurity- expert in om de aard van de dreiging te beoordelen. • Volg de procedures in de planvorming (zorgcontinuïteitsplan).
2 tot 8 uur	
• Verstoring van essentiële zorgprocessen zoals medicatiebeheer en patiëntdossiers. • Mogelijk verdere verspreiding van de cyberdreiging in de systemen.	• Werk met offline patiëntendossiers. • Controleer of kritieke apparaten, zoals medische apparatuur, veilig kunnen blijven functioneren. • Communiceer met medewerkers via alternatieve kanalen. • Neem bij knelpunten in de zorgcontinuïteit contact op met de GHOR.
8 tot 24 uur	
• Vertraging in de zorgverlening. • Er ontstaan logistieke problemen.	• Bepaal prioriteiten voor zorgverlening.
24 uur of langer	
• Langdurige knelpunten in zorgcontinuïteit. • Kwetsbare groepen kunnen getroffen worden.	• Overweeg (gedeeltelijke) evacuatie van kwetsbare patiënten naar andere locaties met volledig functionerende systemen.

Wie doet wat?

- De Veiligheidsregio Brabant-Zuidoost verzorgt crisiscommunicatie, vooral gericht op informatievoorziening, het bieden van handelingsperspectief en duiding.
- GHOR Brabant-Zuidoost inventariseert de getroffen zorginstellingen, legt contact en brengt knelpunten in kaart om zo de regionale zorgcontinuïteit te monitoren.
- De politie heeft een rol in de opsporing van cybercriminelen en werkt hierbij samen met nationale en internationale partners om daders te identificeren en vervolgen. Daarnaast heeft de politie ook een reguliere verantwoordelijkheid ten aanzien van de openbare orde.