COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Eerste Hulp Bij Cybercrises

(TWEE pagina's! Bedoeld gebruik: invullen en bewaren buiten de infrastructuur van de organisatie. Moet ook beschikbaar zijn als je eigen infrastructuur niet beschikbaar is. Bijvoorbeeld: dubbelzijdig afdrukken en veilig bewaren, digitaal in een aparte cloudopslag)
Bij dit document is gebruik gemaakt van het 'kaartje in de meterkast' van de InformatieBeveiligingsDienst en de 'CyberToolkit' van het Digital Trust Center.

De gegevens in dit document zijn voor het laatst gecontroleerd op: dd-mm-jjjj

Belangrijke telefoonnummers

Naam persoon of organisatie	Contactgegevens	24x7?	Toelichting
Collega 1			Crisisorganisatie
Collega 2			Crisisorganisatie
Collega 3			IT helpdesk
Collega 4			Woordvoering/communicatie
			Functionaris gegevensbescherming
Incident respons partner			
Autoriteit Persoonsgegevens	**https://datalekken.autoriteitpersoonsgegevens.nl/**	Ja	Risicovol datalek melden binnen 72 uur, wellicht voormelding doen en later aanpassen.
Z-CERT	**+31 85 070 84 44**	`Ja	Incident melden, ondersteuning bij eerste analyse, doorgeven details om incidenten bij andere zorgaanbieders te voorkomen. Z-CERT brengt u desgewenst in contact met de juiste teams bij de politie om efficiënt aangifte te kunnen doen.
(Cyber)verzekering			polisnummer:

Belangrijke documenten

Document	Versiedatum	Fysieke locatie
Crisishandboek		
Continuïteitsplan & Disaster recoveryplan		
Crisis communicatieplan		
Perslijst		

Stichting Z-CERT
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
KvK 67374972

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Aandachtsgebieden crisisorganisatie

Besteed aan onderstaande thema's voldoende aandacht in de crisisorganisatie. Zo verklein je de kans op onnodige extra verstoringen. Voorbeeld: als je niet je eigen boodschap vertelt aan de media, is de kans groot dat er een verhaal ontstaat waartegen je je moet gaan verdedigen.

Aandachtsgebied	Voorbeelden (niet uitputtend!)
Veiligheid patiënten/cliënten, continuïteit zorg	Altijd prio 1, regelmatig controleren of er veranderingen zijn, afwegingen documenteren. Hulp andere zorginstellingen nodig? – wat kunnen zij bieden? Informeren betrokkenen indien datalek.
(herstel van) systemen	Voorkom verdere verspreiding van het incident. Wat is nodig voor systeemherstel? Acties voor instelling en/of SaaS leverancier? Afhankelijkheden tussen systemen?
Informatie naar toezichthouders	Raad van Toezicht. Autoriteit Persoonsgegevens, Inspectie Gezondheidszorg en Jeugd, Tijdig informeren, beperkte info, inhoud en proces, volgende informatiemoment. Politie? Is er bestaand aangiftebeleid!?
Reputatie /media	Niets zeggen gaat tegenwerken. “dat weten we op dit moment nog niet” is ook een antwoord, inhoud en proces, volgende informatiemoment laten weten. FAQ op website voor diverse doelgroepen. Inspiratie op: https://www.cert.govt.nz/business/guides/communicating-a-cyber-security-incident/public-communications-for-cyber-security-incidents-a-framework-for-organisations/
Interne communicatie	Benoem ook (on)gewenst gedrag op social media, laat bij vragen van buiten naar officiële kanalen verwijzen.
Kosten minimalisatie	Ook bij losgeld betalen heb je aanvullende kosten, intern en extern. Indien van toepassing verzekering tijdig informeren. Onderhandel NIET zelf met gijzelnemers. Hebben anderen meer ervaring mee.
Oorzaak achterhalen	Is in beginfase tot bepaalde hoogte nodig om vervolgacties te bepalen. In later stadium voor aansprakelijkheid en/of vervolging. Let op dat je geen info verwijdert die nog relevant kan zijn; documentatie van keuzes maar ook geheugen van hardware! Het is in dit opzicht vrijwel altijd beter om netwerkverbindingen te verbreken dan systemen uit te zetten.
Tegenstanders leren kennen	Een boze patiënt, cliënt of verwant heeft andere belangen dan een cybercrimineel. Tussen ransomware-groeperingen bestaan verschillen qua aanvalstechniek, betrouwbaarheid in afspraken en mogelijkheden tot onderhandelen. Aanvalstechnieken op https://attack.mitre.org/

Crisisoverleg: Agenda volgens BOB (beeldvorming, oordeelsvorming, besluitvorming) of BOBOC (Beeld, Opties, Besluiten, Opdrachten, Controle). Bijhouden logboek is essentieel. Heb oog voor de fitheid van betrokken personeel!

Stichting Z-CERT
Stationsplein 121
3818 LE Amersfoort
+31 (0)33 737 06 09
info@z-cert.nl
www.z-cert.nl
KvK 67374972