Informatieveiligheid

Business Continuïteitsplan ROHA-praktijken

DIT IS EEN TEMPLATE CONTINUÏTEITSPLAN ALS ONDERDEEL VAN DE ROHA INFORMATIEVEILIGHEIDSSTANDAARDS VOOR DE HUISARTSPRAKTIJKEN

Ben Stoltenborg
Security Officer
01-03-2025

Inhoud

Inleiding

Belang informatieveiligheid

De continuiteit van de zorg en de informatievoorziening is een belangrijk onderdeel van de informatieveiligheid.

Informatieveiligheidsnorm

De NEN7510 norm schrijft voor dat de praktrijk haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties moet vaststellen en de vastgestelde en geïmplementeerde beheersmaatregelen t.b.v. informatiebeveiligingscontinuïteit regelmatig moet verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.

Dit betekent dat de praktijk een actueel overzicht heeft van:

1. Meest reële verstoringen;
2. Maatregelen om de risico's te verminderen;
3. Herstelscenario's;
4. Overzicht van relevante contactpersonen bij verstoringen.

Doel van het document

Om onderdeel te (kunnen) zijn van het ROHA ISMS, en daarmee ook te voldoen aan de informatieveiligheidsnormen NEN7510, dienen de praktijken invulling en/of uitvoering te geven aan een Business Continuïteitsplan (BCP). Dit document is een standaard/template BCP per praktijklocatie met standaard herstelplannen/werkwijzen bij de meest voorkomende verstoringen.

Instructies

De praktijken dienen zelf te beoordelen welke calamiteiten relevant zijn, eventueel voor betreffende praktijk specifieke calamiteiten aan te vullen en het plan te complementeren met actuele contactpersonen en telefoonnummers.

Verstoringen, maatregelen en acties

Verstoringen

- **Locatie onbruikbaar.** Vanuit de locatie(s) van de praktijk kan niet meer gewerkt worden (bv brand, natuurramp, neergestort vliegtuig, etc).
- **Kantoorautomatisering valt uit.** Hierdoor worden de volgende processen geraakt: Facilitair, Financiën, HR en ook de mail-faciliteiten zijn dan niet beschikbaar.
- **HIS werkt niet:** Door een calamiteit bij het datacentrum van een van de dienstverleners zijn kritische ICT-gerelateerde bedrijfsmiddelen onbruikbaar. Hierdoor kunnen bedrijf kritische processen geen doorgang vinden.
- **Onvoldoende beschikbaarheid medewerkers:** Als gevolg van een epidemie kunnen > 40% van de medewerkers niet werken. Hierdoor worden de volgende processen geraakt: huisartsenzorg, Facilitair, Financiën, HR.
- **Geen diensten Systeembeheerder:** door omstandigheden valt systeembeheerder uit.
- **Datalek:** Er heeft een datalek plaatsgevonden die in het kader van de AVG gemeld moet worden aan de Autoriteit Persoonsgegevens en die een verstoring van de bedrijfsprocessen kan veroorzaken.
- **Cyberaanval met gegevensinbreuk:** Vanwege een uiteenlopende oorzaak (phishing, ransomeware etc.) wordt de organisatie getroffen door een cyberaanval met gegevensinbreuk. Hierdoor worden er bijvoorbeeld gevoelige gegevens gestolen of wordt er losgeld geëist voor het vrijgeven van data.

Maatregelen

- **Locatie onbruikbaar:**
    - Consulten kunnen, indien noodzakelijk, vanuit collega praktijk, of tijdelijke huisvesting of bij huisarts op privé locatie plaats kunnen vinden waarmee tijd wordt gecreëerd om op zoek te gaan naar nieuwe locatie.
- **Kantoorautomatisering valt uit:**
    - Om deze calamiteit te voorkomen heeft de systeembeheerder bij wie deze dienst is uitbesteed, passende maatregelen genomen. Hierover zijn afspraken gemaakt en vastgelegd in het contract/SLA.
- **Datacentrum onbruikbaar:**
    - Om deze calamiteit te voorkomen heeft de hostingprovider passende maatregelen genomen. Hierover zijn afspraken gemaakt en vastgelegd in het contract/SLA.
- **Onvoldoende beschikbaarheid medewerkers:**
    - Er zijn afspraken gemaakt met leverancier(s) voor waarneem en invalkrachten.
- **Geen diensten Systeembeheerder:**

- ROHA heeft gelijksoortige afspraken gemaakt met drie systeembeheerders die diensten van elkaar kunnen overnemen.

- **Datalek:**
  - **Maatregelen om datalekken in de praktijk te voorkomen:**
    - Periodieke evaluatie van security incidenten (VIM overleg)
    - Bewustwordingsacties van de ROHA worden (op)gevolgd
    - Medewerkers gewezen op de “10 gouden regels”
    - Medewerkers gewezen op de disciplinaire procedure
    - Geheimhouding in arbeidscontracten
    - Een persoonlijk account toegewezen waar mogelijk. Dit maakt het mogelijk om (ongebruikelijke) activiteiten te monitoren
    - Cyberaanval met gegevensinbreuk:
    - Met systeembeheerders afspraken gemaakt m.b.t. up-to-date virusscanners.
    - Aangesloten op besloten IP-VPN netwerk ingericht voor ROHA en de praktijken met één centrale (managed) FireWall.
    - Werken aan bewustwording bij alle medewerkers van de praktijk.

Herstelacties

- **Locatie onbruikbaar:** er wordt vanuit huis gewerkt tot herstelde of nieuwe locatie beschikbaar is en/of er wordt uitgeweken naar collega praktijken in de coöperatie.
- **Kantoorautomatisering valt uit:** Systeembeheerder lost dit op en bij blijvende problemen kan overgeschakeld worden naar andere systeembeheerder; een en ander in overleg met Functionaris ICT van de ROHA.
- **Datacentrum onbruikbaar:** Stem af met functionaris ICT en/of verantwoordelijke contactpersoon van de ROHA om met betreffende dienstverlener tot een zo snel mogelijke, acceptabele oplossing te komen.
- **Onvoldoende beschikbaarheid medewerkers:** bellen met betreffende leverancier(s) voor invalkrachten.
- **Geen diensten Systeembeheerder:** Stem af met functionaris ICT en/of verantwoordelijke/contactpersoon voor systeembeheerder van de ROHA om vervanging te regelen.
- **Datalek:** Bel met Security Officer ROHA.
- **Cyberaanval met gegevensinbreuk:** Bel met Security Officer ROHA.

Contactpersonen en telefoonnummers

Naam	Rol, functie en/of contact bij verstoringen	Telefoonnummer
Miek van Geenhuizen	Security Officer	06 4850 0621
Huib Hoogendijk	ROHA Functionaris ICT	06 5423 0837
	Systeembeheer	
	HIS	
	Facilitair bedrijf	
	Invalkrachten	
	Praktijkbuur	
	Algemeen alarm t.b.v. brand, politie, ambulance	