ONDERZOEKSRAAD
VOOR VEILIGHEID

Patiëntveiligheid bij ICT-uitval in ziekenhuizen

Eric Ettema

Onderzoeker bij de Onderzoeksraad voor Veiligheid

25 juni 2020

Onderzoeksraad voor Veiligheid

Missie	Verbeteren van veiligheid in situaties waarbij burgers voor hun veiligheid afhankelijk zijn van de overheid, bedrijven of instellingen.
Opdracht	Leren van voorvallen om veiligheid te vergroten.
Sectoren en Kennisdomeinen	Sectoren: Scheepvaart, Railverkeer, Luchtvaart, Industrie. Kennisdomein Gezondheid, o.a.: - Sterftecijfers in een ziekenhuis; - Brand operatiekamer; - Forensische zorg en veiligheid.

Patiëntveiligheid bij ICT-uitval in ziekenhuizen

Onderzoeks-proces

Tegenspraak gedurende het gehele proces

- Verkennend onderzoek
- Bepalen focus
- Onderzoek en analyse
- Inzage procedure
- Publicatie rapport
- Opvolging aanbevelingen

Aanleiding voor dit onderzoek

2018

- 26 januari. Radboud UMC. ICT-storing 11 uur.
- 3 juni. IJsselland Ziekenhuis. ICT-storing 12 uur.
- 16 juli. Dijklander Ziekenhuis. ICT-storing 22 uur.
- 23 oktober. Amsterdam UMC. ICT-storing 32 uur.

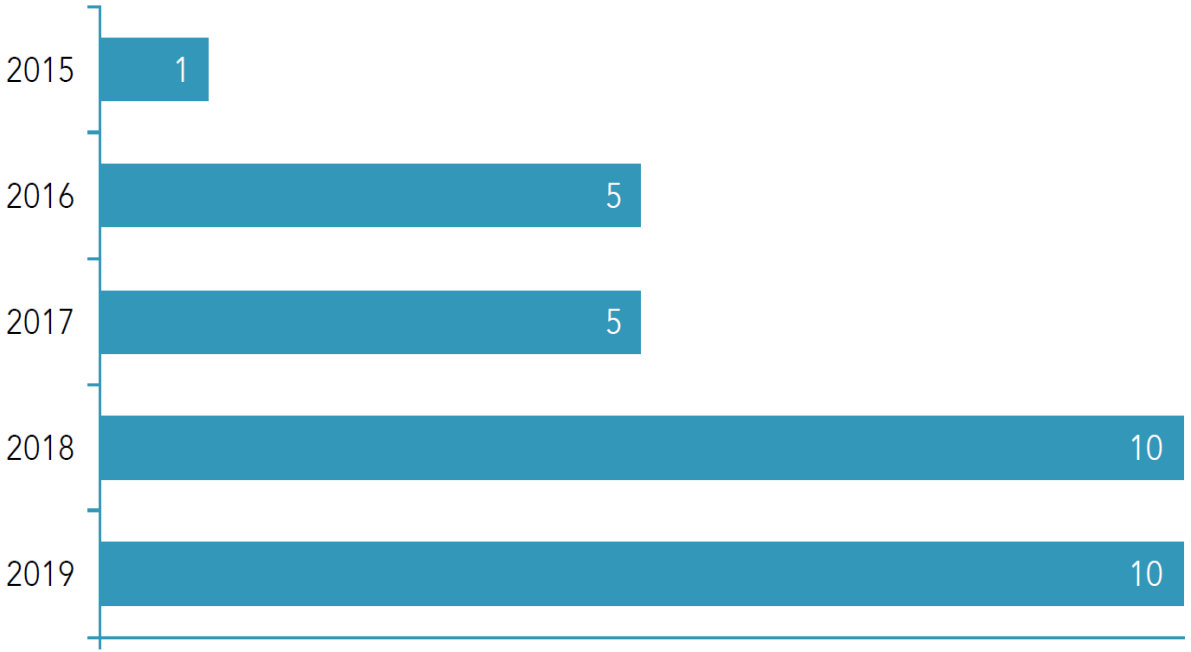
Voorbeelden gevolgen

- EPD's niet beschikbaar; uitval telefonie, printers en alarmsystemen; niet-kunnen opvragen van echo's, röntgenfoto's en scans; uitval laboratoriumsystemen; opnamestop; poli's en OK's dicht; etc.

Digitalisering van de zorg

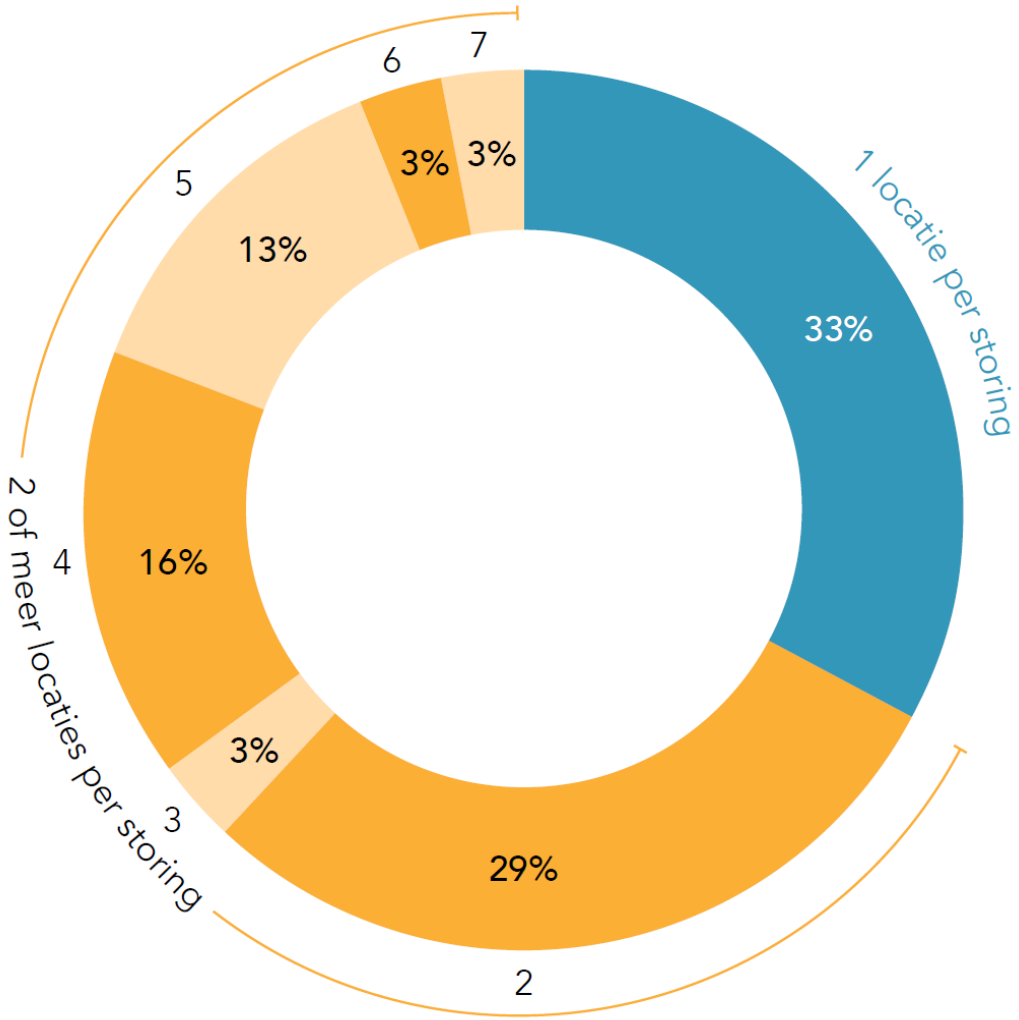
- Zonder ICT geen zorg mogelijk

Hoe vaak doet zich een ICT-storing voor?



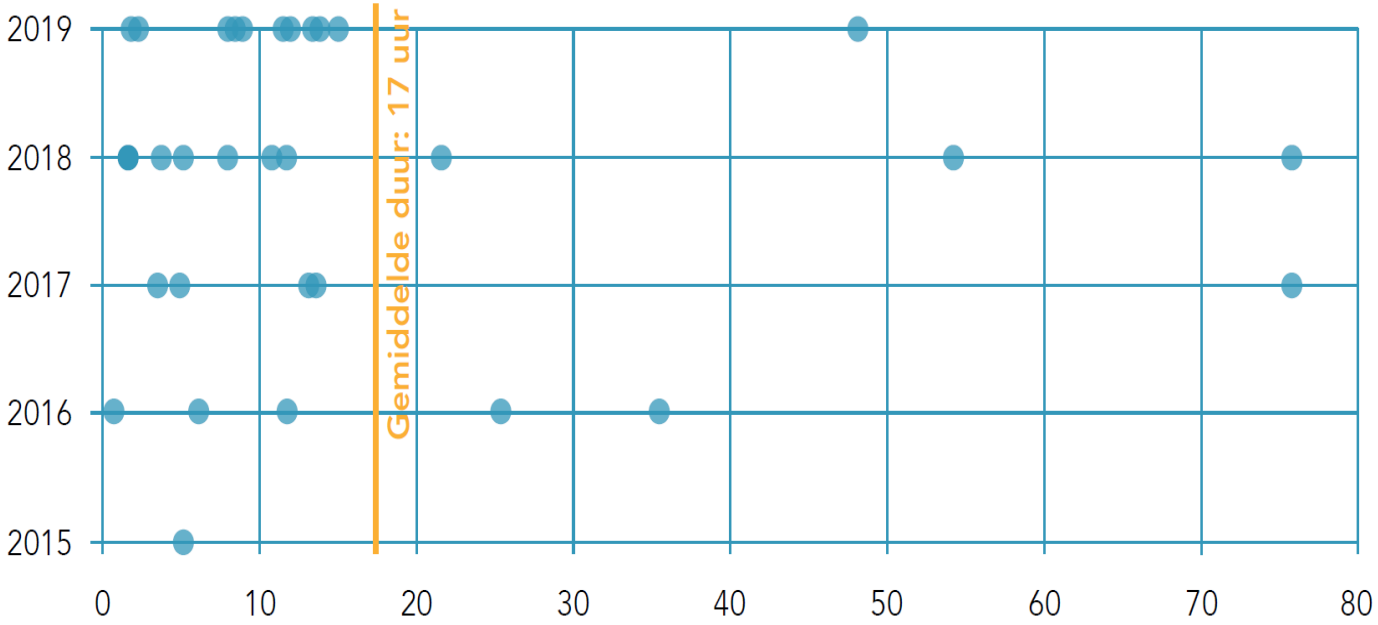
Figuur 1. Aantal ziekenhuizen / ziekenhuisgroepen met een ICT-storing, 2015-2019.

Meerdere locaties per ziekenhuis



Figuur 2. Aantal getroffen ziekenhuislocaties per storing.

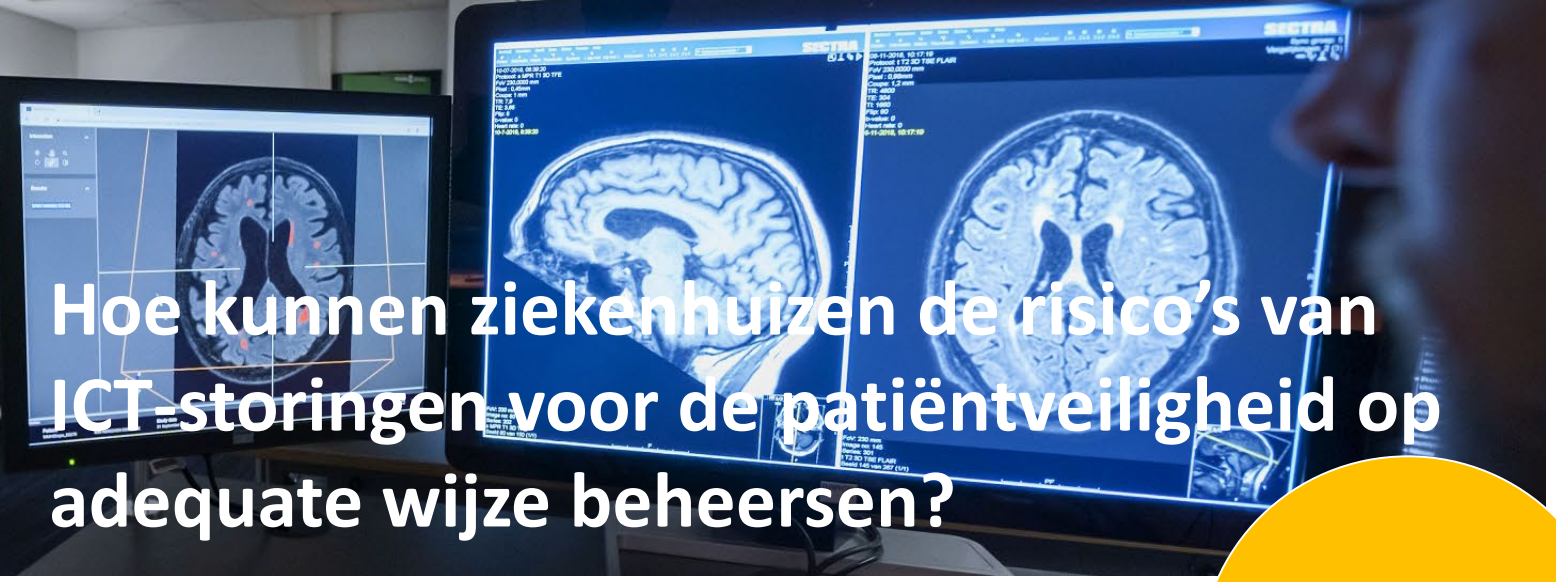
Duur van de storing



Figuur 3: Duur van ICT-storingen in ziekenhuizen in uren, 2015 - 2019.

De Onderzoeksraad vroeg zich af:

In hoeverre brengt ICT-uitval de veiligheid van patiënten in gevaar?



Hoe kunnen ziekenhuizen de risico's van ICT-storingen voor de patiëntveiligheid op adequate wijze beheersen?

Onderzoekopzet

- 6 ICT-storingen onderzocht, waarvan 3 uitgebreid
- Oorzaken, incidentbestrijding en crisisbeheersing
- Logbestanden, verslagen crisis-overleggen, evaluaties
- Interviews betrokkenen, experts, analyse- en focussessies
- (Potentiële) effecten op patiëntveiligheid

In dit webinar drie thema's:

I: Gesignaleerde onvolkomenheden

II: Risico's voor de patiënt

III: Hoe beheers je de risico's?

I: Gesignaleerde onvolkomenheden

1) Inrichting en beheer ICT-fundament

a) Redundante systemen niet afdoende ingericht:
- Wel aanwezig maar (nog) niet ingericht
- Wel ingericht maar toegang nog via primaire systeem
- Wel werkend maar handmatig teruggedraaid

Systeem, inrichting, beheer, afstemming, menselijk handelen

b) Beperkte monitoring van systemen
- Niet overal real time en continue monitoring

c) Tekortkoming in regierol richting externe partijen
- Onduidelijkheden in rollen en verantwoordelijkheden

d) Onvoldoende inrichting change- en incident management
- Beperkingen draaiboek, toezicht, afspraken escalatie

I: Gesignaleerde onvolkomenheden (vervolg)

2) Beperkte voorbereiding op ICT-uitval

a) **Beperkte planvorming**
- Wel ICT-uitval in crisisplan, maar nauwelijks uitwerking

b) **Beperkt opleiden en trainen van crisisfunctionarissen**
- Geen oefeningen met grootschalige ICT-uitval

3) Evaluatie en onderzoek: onvolledig

a) **Beperkt inzicht in directe en achterliggende oorzaken**
- Beperkingen onderzoek, vastlegging, maatregelen

b) **Beperkt inzicht in gevolgen voor patiëntveiligheid**
- Wel schade onderzocht, niet *verhoogde kans* op schade

II: Risico's voor de patiënt

1) Patiëntinformatie niet beschikbaar
   => onzekerheid behandelmogelijkheden
2) Opnamestop
   => langere aanrijdtijden / minder zorgmogelijkheden
3) Communicatiesystemen vallen uit
   => bemoeilijkt gegevensuitwisseling en alarmering
4) Terugvallen op papier
   => zoekraken van informatie, verkeerd interpreteren
5) Terugval in efficiëntie
   => tijdige zorg onder druk
6) Vermoeidheid en stress
   => sneller maken van fouten
7) Medische apparatuur valt uit / stand alone modus
   => beperkt diagnosestelling, monitoring, datastroom

Aandacht voor genoemde risico's?

Tijdens incident veel aandacht voor patiëntveiligheid

1) Overschakelen op noodprocedures
2) Sterk vertrouwen op veerkracht
3) Opnamestop om veiligheid patiënten te waarborgen

Na afloop beperkte beeldvorming van risico's voor patiënt

1) Verhoogde *kans op schade* nauwelijks in beeld
2) Geen diepgaande analyse gevolgen voor patiëntveiligheid
3) Schade aan uitgeweken patiënten beperkt in beeld

Beperkte beeldvorming beperkt ziekenhuizen te leren van voorvallen en adequate beheersmaatregelen te nemen.

III: Hoe beheers je de risico's?

1) Zorg voor organisatiebreed risicobesef

=> nodig om risico's te vertalen in beheersmaatregelen

=> besef dat patiëntveiligheid in het geding is geweest

=> dit is ook belangrijk i.v.m. kwetsbaarheid andere partijen

Uitwerking van risico's ICT-uitval nodig voor adequate beheersing.

2) Zorg voor bestuurlijke aandacht

=> Ziekenhuis: EPD, pt-zorg, netwerksamenwerking, financiën.

=> ICT-thema's: gegevensuitwisseling, cybercrime, datalekken.

=> IGJ: toetsing e-health, convenant medische technologie.

Meer aandacht nodig voor risico's van niet-intentionele ICT-uitval.

III: Hoe beheers je de risico's? (vervolg)

3) **Zorg voor veerkracht én voorbereiding**

=> ziekenhuizen zien veerkracht personeel als beheersmaatregel.

=> maar veerkracht is beperkt én veel zorgprocessen digitaliseren.

=> goede beheersing van risico's is afhankelijk van voorbereiding.

Breng ICT-afhankelijkheden in kaart, doordenk gevolgen voor patiënt en zorg voor O.T.O . van personeel in het omgaan ICT-uitvalscenario's.

4) **Breng de werelden van zorg en ICT bij elkaar**

=> CMIO, CNIO: aandacht voor risico's ICT-uitval.

=> VIM-analyse: ICT-inbreng.

=> PRI: ook bij softwaretoepassingen en wijziging ICT-fundament.

=> Crisisorganisatie: samenwerking zorg en ICT (voorbereiding en bestrijding van ICT-uitval vanuit de gevolgen voor patiënt).

Zorg voor adequate inbedding van de samenwerking tussen zorg-ICT.

Conclusies

- Digitalisering is doorgedrongen tot het hart van de zorg.
- Ziekenhuizen zijn daardoor toenemend afhankelijk van ICT.
- Uitval van ICT kan grote gevolgen hebben voor de patiënt.
- Bewustwording hiervan blijft achter bij de ICT-afhankelijkheid.
- Adequate risicobeheersing vereist meer aandacht voor het voorkomen en bestrijden van ICT-uitval en voor de gevolgen van ICT-uitval voor de patiëntveiligheid.

Aanbevelingen aan NVZ en NFU (verkort)

1. Bewerkstellig dat uw leden:

a. De afhankelijkheden tussen zorg en ICT periodiek in kaart brengen, inclusief de mogelijke risico's voor patiënten.

b. Periodiek de ICT-systemen in samenhang testen. Ook dient geoefend te worden met scenario's waarbij de ICT uitvalt. Betrek leveranciers bij deze oefeningen en testen.

c. Na elke ernstige ICT-uitval evaluaties uitvoeren waarbij ook de (verhoogde kans op) schade voor zowel in-huis patiënten als uitgeweken patiënten diepgaand wordt geanalyseerd.

Aanbevelingen aan NVZ en NFU (vervolg)

2. Borg dat ziekenhuizen dit vraagstuk gezamenlijk benaderen en van en met elkaar leren.

3. Ontwikkel een praktisch handvat voor ziekenhuizen voor het beheersen van de risico's van uitval van ICT.

4. Ga in regionaal verband na of in geval van ICT-uitval waarbij meerdere ziekenhuislocaties in een regio worden getroffen, de veiligheid van patiënten voldoende is geborgd.

Aanbeveling aan IGJ

5. Besteed in het toezicht op ziekenhuizen aandacht aan de punten in bovengenoemde aanbevelingen.


Het volledige rapport is te vinden op:
https://www.onderzoeksraad.nl/nl/page/4980/patiëntveiligheid-bij-ict-uitval-in-ziekenhuizen