Implementatie van NIS2

Hoe kan de cyberweerbaarheid van CSA versterkt worden in het kader van de NIS2 richtlijn?

AZ Klina
voluit voor zorg

Inleiding

AZ Klina
voluit voor zorg

Waarom werd NIS2 ingevoerd?

- 2016: NIS1
  - Eerste Europese cyberwet

↓

- Digitale evolutie
  - Meer digitalisering in ziekenhuizen
  - Toename ransomware-aanvallen
  - Grotere afhankelijkheid van IT-systemen

↓

- 2023: NIS2-richtlijn
  - Strengere cybersecurity-eisen
  - Meer aandacht voor risicobeheer, bedrijfscontinuïteit en opleiding & awareness

↓

- 2024: Omzetting naar nationale wetgeving

AZ Klina
voluit voor zorg

Wat is het doel van NIS2?

- **Cyberbeveiliging** en de **weerbaarheid** van kritieke en essentiële entiteiten in diverse sectoren **versterken**
  - Ziekenhuis = essentiële entiteit

- Voor 18 april 2027 moeten alle ziekenhuizen aantonen dat zij voldoen aan de NIS2-vereisetn en cyberrisico's actief beheersen

- Concreet:
  - Cyberrisico's identificeren en beperken
  - Incidenten snel detecteren en melden
  - Kritieke processen operationeel houden
  - Medewerkers opleiden en sensibiliseren
  - De impact van cyberaanvallen minimaliseren

AZ Klina
voluit voor zorg

NIS2 domeinen

NIS2 domein	Voorbeeld in de ziekenhuisapotheek
Risicobeheer	Kritische processen bij IT-uitval identificeren
Cyberawareness	Phishing herkennen en verdachte e-mails melden
Incidentmanagement	Procedures bij cyberincidenten
Bedrijfscontinuïteit	Werken volgens downtimeprocedures
Leveranciersbeheer	Sterilisatiesoftware en externe diensten
Toegangsbeveiliging	Sterke wachtwoorden & MFA
Evaluatie & verbetering	Oefeningen en testen van noodprocedures

AZ Klina
voluit voor zorg

Praktische invulling van NIS2

- A. Risico-analyse
  - Kritische processen identificeren
  - Impact van IT-uitval beoordelen
  - Kwetsbaarheden in kaart brengen
- B. Awareness en opleiding
  - Phishing herkennen
  - Veilige wachtwoorden gebruiken
  - Cyberincidenten melden
- C. Bedrijfscontinuïteit
  - Downtimeprocedures uitwerken
  - Kritische zorgprocessen operationeel houden



AZ Klina
voluit voor zorg

A. Risico-analyse

Praktische uitwerking

AZ Klina
voluit voor zorg

Welke risico's zien we binnen CSA?

- Voorbeeld kritische processen
  - Flow reinigen ➜ samenstellen/inpakken ➜ steriliseren
  - Traceerbaarheid van instrumenten
  - Vrijgave van steriel materiaal
  - Communicatie met OK
  - Voorraadbeheer

- Mogelijke gevolgen van IT-uitval
  - Geen toegang tot samenstelling sets
  - Werken toestellen nog zonder netwerk?
  - Geen toegang tot sterilisatiegegevens
  - Verlies van traceerbaarheid
  - Vertraging van operaties
  - Handmatige werkwijzen noodzakelijk
  - Impact op continuïteit van zorg en patiëntveiligheid

AZ Klina
voluit voor zorg

Stapsgewijze aanpak

- Stap 1: kritische processen identificeren
  - Alle processen in kaart brengen
  - Impact van IT-uitval beoordelen
- Stap 2: Risico's analyseren (HFMEA-methode)
  - Mogelijke storingen identificeren
  - Ernst, frequentie en detecteerbaarheid beoordelen
- Stap 3: Verbetermaatregelen uitwerken
  - Gap-analyse uitvoeren: kloof tussen huidige en gewenste situatie
  - Verbetermaatregelen implementeren: risico's verminderen
  - Opnieuw evalueren

➔ Resultaat: inzicht in de meest kritische processen

AZ Klina
voluit voor zorg

B. Awareness en opleiding

AZ Klina
voluit voor zorg

Waarom zijn awareness en opleiding belangrijk?

- De mens is vaak de **laatste verdedigingslinie**
  - Cyberincidenten ontstaan niet alleen door technische problemen
  - Onbedoelde menselijke fouten vormen een belangrijke oorzaak van cyberincidenten
  - Eén klik op een phishingmail kan de werking van een ziekenhuis verstoren
- **Kennis en bewustzijn** zijn cruciaal
  - Verdachte e-mails herkennen
  - Sterke wachtwoorden gebruiken
  - Correct omgaan met gegevens
  - Cyberincidenten tijdig melden
- Cyberveiligheid = **verantwoordelijkheid van iedereen**

AZ Klina
voluit voor zorg

Hoe meten en verbeteren we cyberbewustzijn?

- 1. Meten
  - Mate van bewustwording rond cybersecurity meten bij het personeel via een baseline enquête
- 2. Verbeteren
  - Opleidingen
  - Nieuwsbrieven
  - Sensibiliseringsacties
- 3. Evalueren
  - Identieke tweede enquête
  - Effect van de maatregelen beoordelen

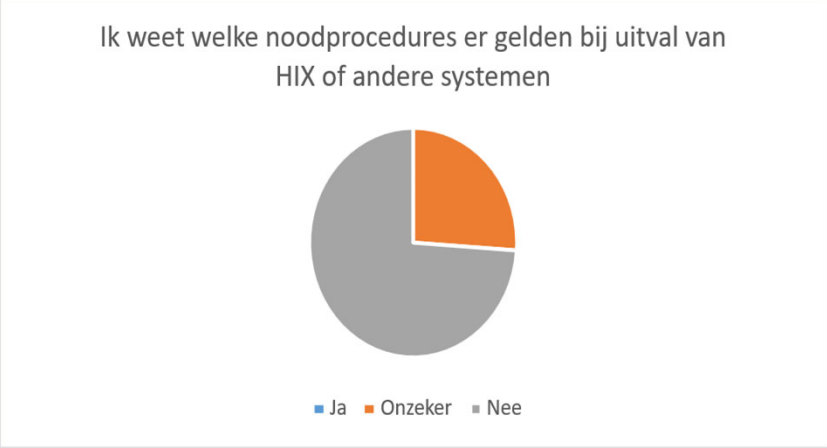
➔Continue verbetering van cyberbewustzijn

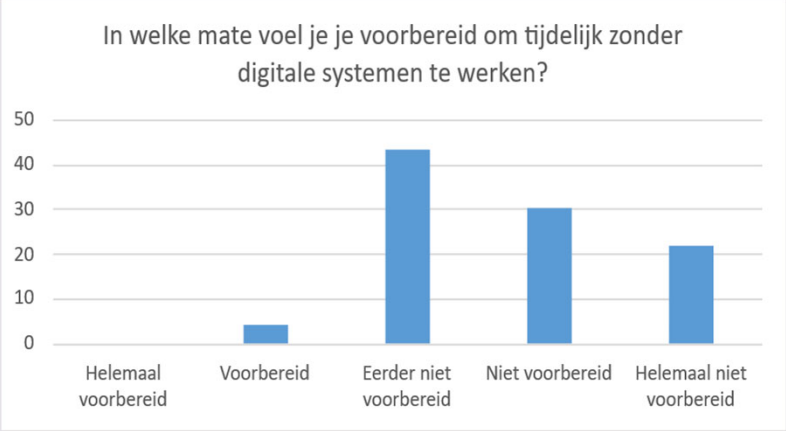
➔Aanpak reeds toegepast bij de ziekenhuisapotheek van AZ Klina

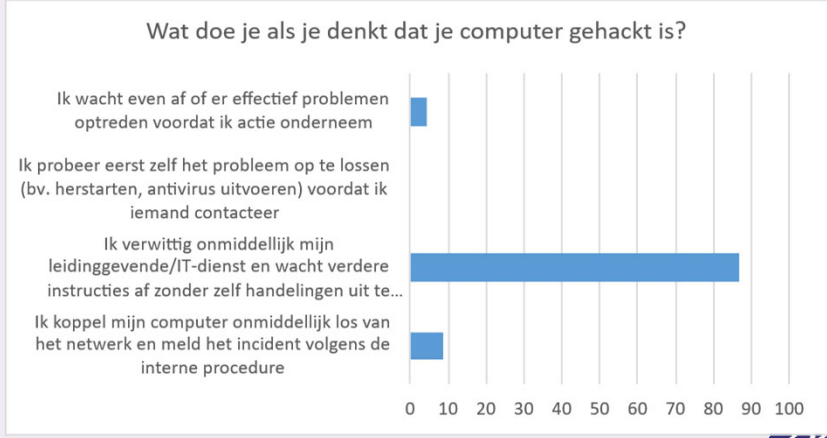
AZ Klina
voluit voor zorg

Wat leerden we uit de enquête?









AZ Klina
voluit voor zorg

Hoe hebben we hierop gereageerd?

PHISHING & E-MAILVEILIGHEID

TRAP NIET IN PHISHING: HERKEN EN REAGEER CORRECT

1) Wat is phishing?

Bij phishing verstuurt de aanvaller een **frauduleuze sms** of **e-mail** namens een ogenschijnlijk betrouwbaar persoon of organisatie. Het doel is om de ontvanger ertoe te verleiden om op een **specifieke link** of **bijlage** te **klikken.** Hierdoor kunnen er inloggegevens of wachtwoorden gestolen worden.

2) Een verdachte e-mail herkennen

Spamfilters of **antivirussoftware** bieden geen volledige bescherming tegen phishing. Waakzaamheid blijft essentieel. Een phishingmail herken je vaak aan volgende signalen:

- **Links of bijlagen:** klik nooit zomaar op links of open geen onbekende bijlagen
- **Onverwacht**: een e-mail zonder duidelijke aanleiding is verdacht
- **Dringende toon:** berichten die druk creëren vragen extra alertheid
- **Afzender:** controleer het e-mailadres zorgvuldig, vaak lijkt het sterk op een officieel e-mailadres

Opgelet: phishingmails bevatten tegenwoordig **weinig of geen taalfouten** dankzij AI

3) Gedrag bij een verdachte e-mail

Open geen bijlagen en klik niet op links in verdachte berichten. Bijlagen kunnen **malware** bevatten. Dit is schadelijke software die niet alleen je eigen apparaat, maar ook het hele bedrijfsnetwerk kan **infecteren**.

Wanneer je denkt dat je een phishing bericht hebt ontvangen, dan is het belangrijk om het bericht **onmiddellijk te melden**.

Wat je zeker **niet** moet doen:

- antwoorden op verdachte e-mails
- zelf op onderzoek gaan door op links te klikken/bijlagen te openen
- gevoelige informatie delen via e-mail



4) Bewustwording in de praktijk

Binnen AZ Klina worden verschillende initiatieven ingezet om het bewustzijn rond phishing te versterken. Zo ontvangen medewerkers **maandelijks testmails** om te evalueren in welke mate phishingpogingen correct herkend worden. Wanneer een dergelijke e-mail wordt ontvangen, wordt verwacht dat medewerkers deze niet enkel verwijderen, maar ook **rapporteren** via het **'phished'-icoon**.

Daarnaast biedt de **Phished Academy** korte online opleidingen aan over onder meer veilig e-mailverkeer en andere thema's binnen de NIS2-richtlijn. De modules duren slechts 5 tot 10 minuten en zijn gemakkelijk tussendoor te volgen. je kan eenvoudig inloggen met je Klina-account.

5) Interne procedure AZ Klina

Een verdachte e-mail kan je melden door op de knop 'Phished' rechtsboven in de e-mail te klikken. Het Phished Team onderzoekt eerst of het om een testmail gaat. Is dat niet het geval, dan neemt IT de melding verder in behandeling. Het is belangrijk om in tussentijd **niets met de e-mail te doen.** De e-mail wordt geanalyseerd en nadien ontvang je een bericht met de resultaten van het onderzoek en de bevestiging of de e-mail al dan niet veilig is.

6) Ga zelf aan de slag

- **Start met het rapporteren van verdachte e-mails**
- **start met de opleidingen van Phished Academy**

AZ Klina
voluit voor zorg

C. Bedrijfscontinuïteit

Uitwerken van noodprocedures

AZ Klina
voluit voor zorg

Continuïteit van kritische processen

- NIS2 vraagt dat **kritische processen kunnen blijven functioneren** bij IT-uitval

- Voor CSA kan dit onder meer betrekking hebben op:
  - Flow reinigen ➜ samenstellen/inpakken ➜ steriliseren
  - Traceerbaarheid van instrumenten
  - Vrijgave van steriel materiaal
  - Communicatie met het operatiekwartier
  - Beheer van voorraden
  - Toegang tot kritische documenten en gegevens

- Belangrijke vragen
  - Hoe blijven deze processen functioneren bij IT-uitval?
  - Welke informatie moet beschikbaar zijn?
  - Welke alternatieven zijn voorzien indien systemen niet beschikbaar zijn?

AZ Klina
voluit voor zorg

Noodprocedures

- Voor elk kritisch proces worden **noodprocedures** uitgewerkt
- De aanpak hangt af van de **duur van de IT-uitval**
- Een uitval van 3 uur vraagt een andere aanpak dan een uitval van 3 dagen of 3 weken

  - 3 uur → korte verstoring
  - 3 dagen → langdurige verstoring
  - 3 weken → crisismodus

➔ Niet elke IT-uitval vereist dezelfde maatregelen

AZ Klina
voluit voor zorg

Tijdskriticiteit

- Hoe snel moet een proces opnieuw beschikbaar zijn?
- Welke processen kunnen enkele minuten, enkele uren of meerdere dagen uitvallen zonder impact op patiëntveiligheid of continuïteit?

KRITIEK	Opstart binnen minuten noodzakelijk
HOOG	Opstart binnen enkele uren vereist
MATIG	Tijdelijke vertraging mogelijk
LAAG	Kan meerdere dagen wachten

➔ Niet elk proces heeft dezelfde prioriteit tijdens een cyberincident of IT-uitval

AZ Klina
voluit voor zorg

Dankjewel

eindslide

AZ Klina

voluit voor zorg