Hacking Willebroek
25/01/2020
00:22:13

Webinar VVSG:
We worden gehackt. Wat nu?

27/01/2020

da's Willebroek

Gastsprekers

- Eddy Bevers, Burgemeester
- Dirk Blommaert, Algemeen directeur
- Luc Hertmans, Dienst ICT
- Steven Vermeeren, Noodplanningsambtenaar

da's Willebroek

Inhoud

- Informatiedeling
- Bron/oorzaak
- Impact
- Crisisbeheer
- Communicatie
- Recovery

da's Willebroek

ANTWERPEN

Gemeentediensten van Willebroek slachtoffer van cyberaanval: "Hackers vragen betaling in bitcoins"

TECHNOLOGIE

"In 2021 gaan we nog meer cyberaanvallen krijgen": vanwaar komen die aanvallen? En hoe kan je jezelf beschermen?

ANTWERPEN

Cyberaanval treft AP Hogeschool: alle campussen hele dag gesloten

BINNENLAND

Winkelketen Aveve is slachtoffer van cyberaanval

Bedrijven betalen steeds vaker "losgeld" aan hackers die systemen platleggen met ransomware of gijzelingssoftware, schrijft cybersecurityspecialist Arnout Van de Meulebroucke. En dat moedigt die cybercriminelen aan, terwijl we net meer zouden moeten doen om hen te ontmoedigen.

OOST-VLAANDEREN

Cyberaanval op Arteveldehogeschool: ICT'ers in volle strijd tegen digitale criminelen

op vliegtuigbouwer Asco

WEST-VLAANDEREN

Financiële schade na cyberaanval Picanol blijkt beperkt, bedrijf heeft ook géén losgeld betaald

CORONACRISIS

Cyberaanval op Europees Geneesmiddelenbureau: documenten over coronavaccin van Pfizer/BioNTech ingekeken

da's Willebroek

Doel van bij het begin

- Continuïteit dienstverlening
- Open blijven
- Motiveren/inspireren team
- Technisch verhaal
- Betaling

da's Willebroek

Informatiedeling

Er is een uitgebreid rapport opgemaakt. Dit rapport werd donderdag 5 maart voorgesteld op het kabinet van minister Somers.

Dit rapport heeft tot doel het incident 'cyber-aanval Willebroek' te documenteren, meer specifiek:

- het beschrijven van de bron
- het beschrijven van de impact
- het beschrijven van de crisisbeheerstructuur
- het beschrijven en documenteren van instructies aan personeel / externen
- het beschrijven van de interne en externe communicatie
- het aanreiken van nuttig documenten: FAQ, persberichten, tijdslijn,…

met als doel:

- het documenteren van de aanpak als leidraad bij herhaling
- het formuleren van verbeterpunten
- het ter beschikking stellen aan externe besturen/instellingen ter inspiratie bij het opstellen van INP'en

da's Willebroek

Bron / Oorzaak

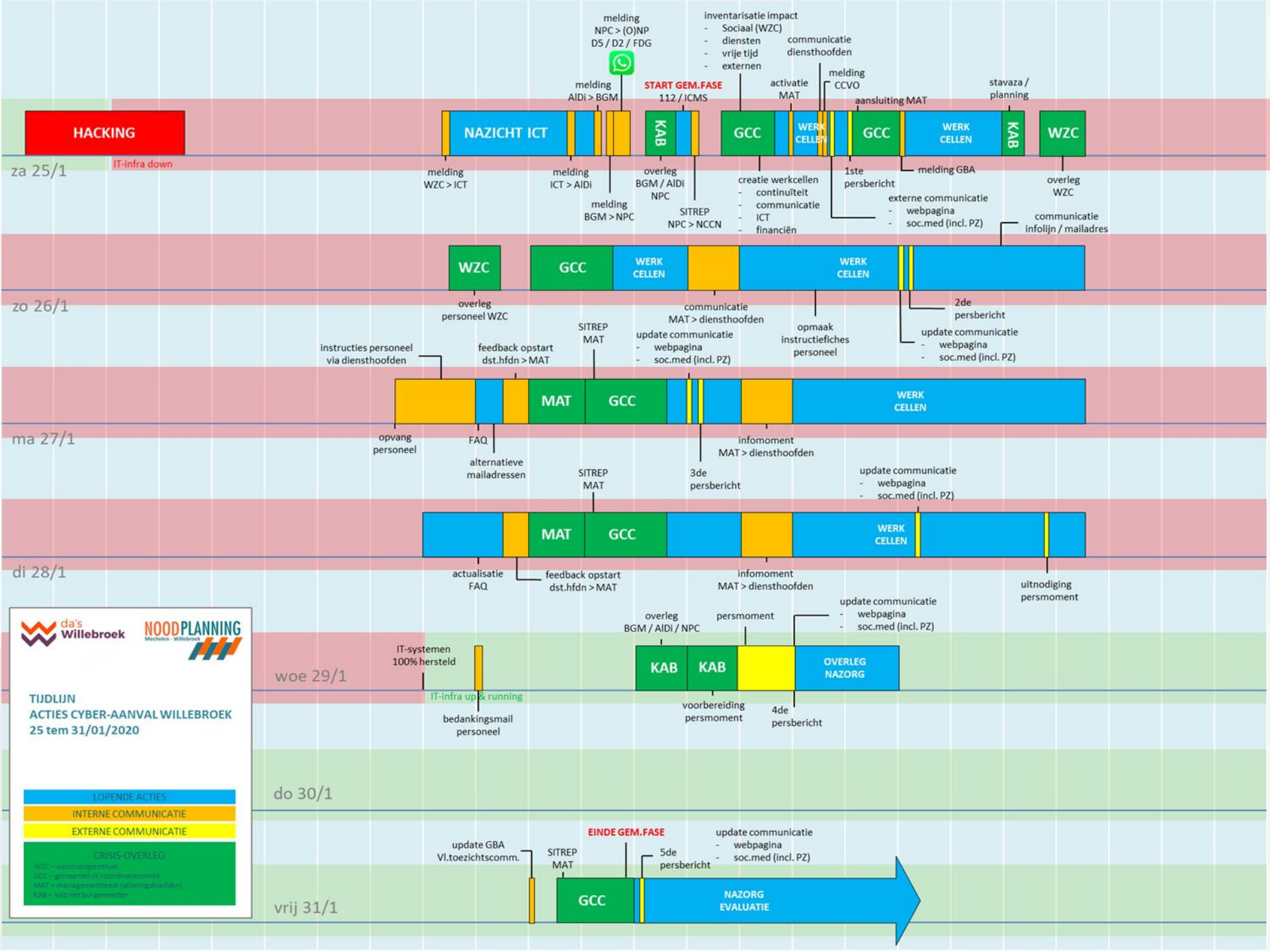
- Actieve aanval / inbraak
  - Recente vunerability op onze SSL appliance
  - Inbraak via laatste accounts die de SSL gebruikten
  - RDP naar server Anti-virus om die te saboteren
  - RDP naar andere servers + loslaten ransomware
- Strategisch moment
  - Zaterdag morgen 25/01/2020 om 00:22:13
  - Weekend = weinig of geen activiteit
- Vaststelling
  - Woonzorgcentrum zit mee op ons netwerk – activiteit 24/24 7/7
  - Zaterdagmorgen melding aan ICT dat gegevens rusthuisbewoners niet consulteerbaar zijn
  - Eerste onderzoek ICT (vermoedelijk oorzaak binnen gebruikte applicatie)
  - Echter vaststelling dat bepaalde data zijn geëncrypteerd + vondst ransomnote
  - Vaststelling dat ook andere servers geïmpacteerd waren
  - Eerste voorzichtige inschatting downtime : 1 week

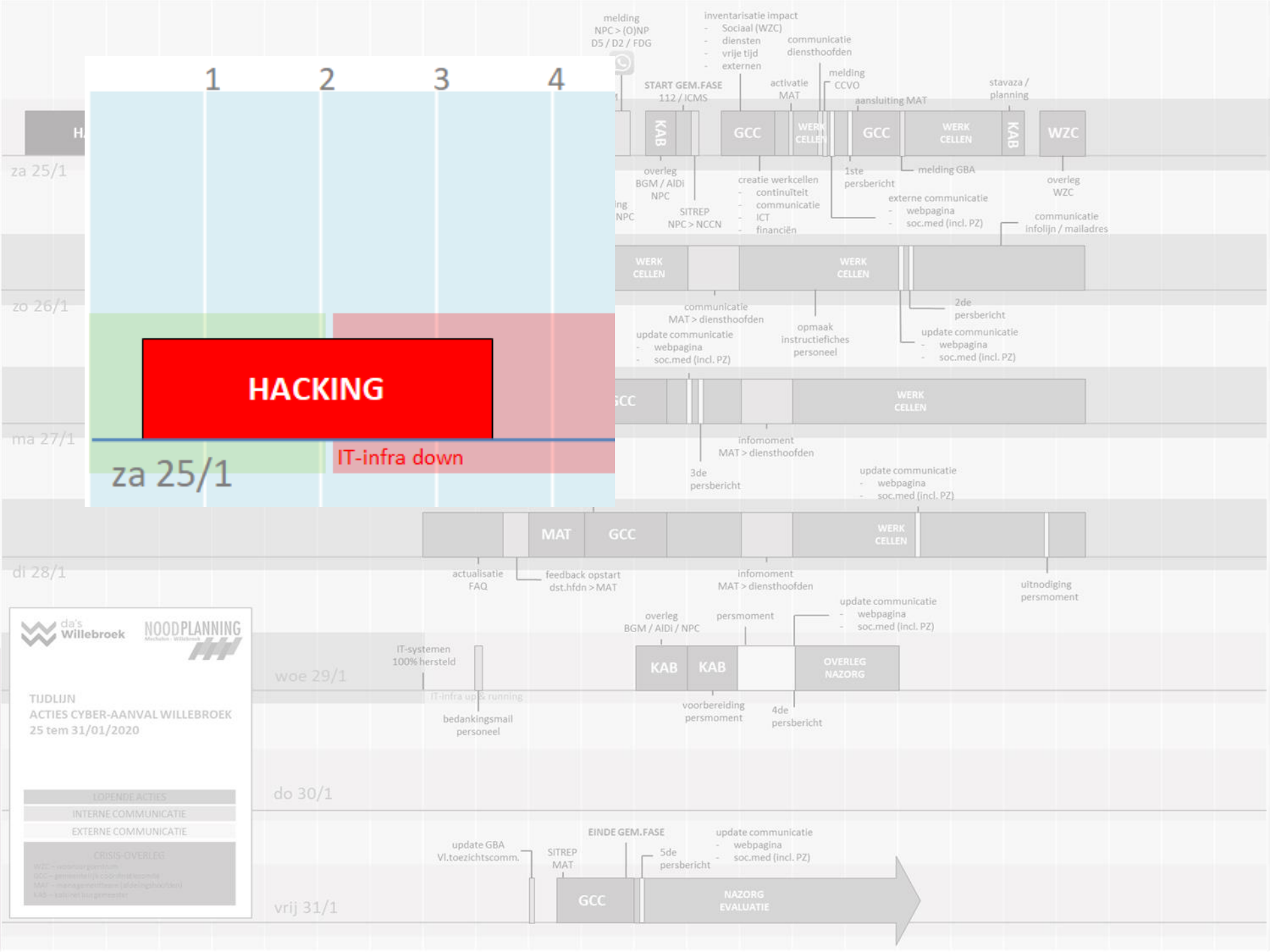
da's Willebroek

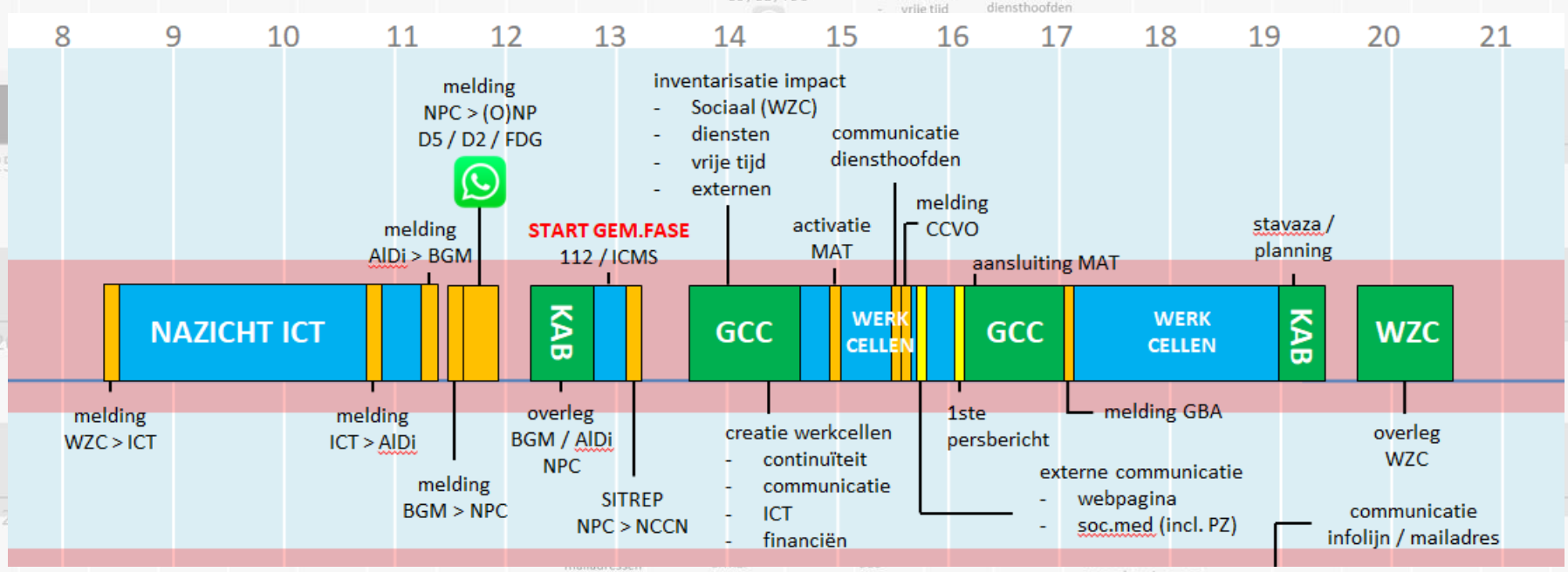
Bron / Oorzaak / acties

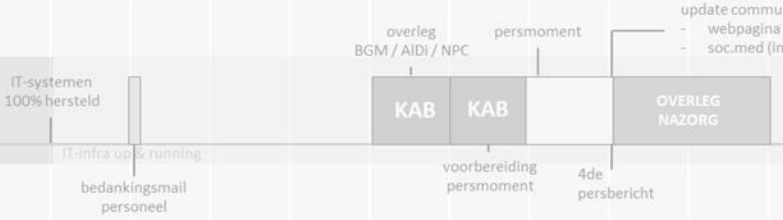
- Eerste acties
  - Netwerk werd geïsoleerd – backups worden stopgezet
  - AD en Burgemeester worden ingelicht.
  - Politie en Parket worden ingelicht alsook noodplanambtenaar.
  - Gemeentelijke crisis cel komt samen.
  - Open communicatie naar de buitenwereld.
  - Reeds zaterdag eerste onderzoek met LCCU en specialist van firma Secutec.
  - Zondag verder federaal onderzoek met 4 onderzoekers van de FCCU
    - Wat – wanneer – wie – waar - ….via onderzoek logfiles
    - Is er nog iets actief van de malware ?
    - Blokkeren van alle mogelijk betrokken accounts
  - Extra monitoring van extern verkeer wordt reeds opgezet via secutec (secure DNS)
  - ICT test eerste restore van backup in geïsoleerde omgeving.

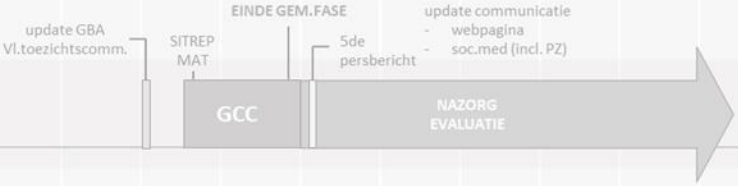
da's Willebroek


da's Willebroek
NOODPLANNING
Mechelen - Willebroek
TIJDLIJN
ACTIES CYBER-AANVAL WILLEBROEK
25 tem 31/01/2020
LOPENDE ACTIES
INTERNE COMMUNICATIE
EXTERNE COMMUNICATIE
CRISIS-OVERLEG
WZC – woonzorgcentrum
GCC – gemeentelijk coördinatiecomité
MAT – managementteam (afdelingshoofden)
KAB – kabinet burgemeester
za 25/1
zo 26/1
ma 27/1
di 28/1
woe 29/1
do 30/1
vrij 31/1
HACKING
IT-infra down
NAZICHT ICT
KAB
GCC
WERK CELLEN
WZC
MAT
OVERLEG NAZORG
NAZORG EVALUATIE
melding NPC > (O)NP D5 / D2 / FDG
melding AIDi > BGM
START GEM.FASE 112 / ICMS
inventarisatie impact
- Sociaal (WZC)
- diensten
- vrije tijd
- externen
communicatie diensthoofden
activatie MAT
melding CCVO
aansluiting MAT
stavaza / planning
melding WZC > ICT
melding ICT > AIDi
melding BGM > NPC
overleg BGM / AIDi NPC
SITREP NPC > NCCN
creatie werkcellen
- continuïteit
- communicatie
- ICT
- financiën
1ste persbericht
melding GBA
externe communicatie
- webpagina
- soc.med (incl. PZ)
overleg WZC
communicatie infolijn / mailadres
overleg personeel WZC
communicatie MAT > diensthoofden
opmaak instructiefiches personeel
2de persbericht
update communicatie
- webpagina
- soc.med (incl. PZ)
instructies personeel via diensthoofden
feedback opstart dst.hfdn > MAT
SITREP MAT
update communicatie
- webpagina
- soc.med (incl. PZ)
opvang personeel
FAQ
alternatieve mailadressen
3de persbericht
infomoment MAT > diensthoofden
SITREP MAT
update communicatie
- webpagina
- soc.med (incl. PZ)
actualisatie FAQ
feedback opstart dst.hfdn > MAT
infomoment MAT > diensthoofden
uitnodiging persmoment
IT-systemen 100% hersteld
IT-infra up & running
bedankingsmail personeel
overleg BGM / AIDi / NPC
persmoment
update communicatie
- webpagina
- soc.med (incl. PZ)
voorbereiding persmoment
4de persbericht
update GBA Vl.toezichtscomm.
SITREP MAT
EINDE GEM.FASE
5de persbericht
update communicatie
- webpagina
- soc.med (incl. PZ)


1
2
3
4
HACKING
IT-infra down
za 25/1
za 25/1
zo 26/1
ma 27/1
di 28/1
woe 29/1
do 30/1
vrij 31/1
melding NPC > (O)NP D5 / D2 / FDG
inventarisatie impact
- Sociaal (WZC)
- diensten
- vrije tijd
- externen
communicatie diensthoofden
melding CCVO
START GEM.FASE 112 / ICMS
activatie MAT
aansluiting MAT
stavaza / planning
KAB
GCC
WERK CELLEN
GCC
WERK CELLEN
KAB
WZC
overleg BGM / AIDi NPC
SITREP NPC > NCCN
creatie werkcellen
- continuïteit
- communicatie
- ICT
- financiën
1ste persbericht
melding GBA
externe communicatie
- webpagina
- soc.med (incl. PZ)
overleg WZC
communicatie infolijn / mailadres
WERK CELLEN
WERK CELLEN
communicatie MAT > diensthoofden
update communicatie
- webpagina
- soc.med (incl. PZ)
opmaak instructiefiches personeel
2de persbericht
update communicatie
- webpagina
- soc.med (incl. PZ)
WERK CELLEN
infomoment MAT > diensthoofden
3de persbericht
update communicatie
- webpagina
- soc.med (incl. PZ)
MAT
GCC
WERK CELLEN
actualisatie FAQ
feedback opstart dst.hfdn > MAT
infomoment MAT > diensthoofden
uitnodiging persmoment
overleg BGM / AIDi / NPC
persmoment
update communicatie
- webpagina
- soc.med (incl. PZ)
IT-systemen 100% hersteld
IT-infra up & running
KAB
KAB
OVERLEG NAZORG
bedankingsmail personeel
voorbereiding persmoment
4de persbericht
update GBA Vl.toezichtscomm.
SITREP MAT
EINDE GEM.FASE
5de persbericht
update communicatie
- webpagina
- soc.med (incl. PZ)
GCC
NAZORG EVALUATIE
da's Willebroek
NOODPLANNING
TIJDLIJN
ACTIES CYBER-AANVAL WILLEBROEK
25 tem 31/01/2020
LOPENDE ACTIES
INTERNE COMMUNICATIE
EXTERNE COMMUNICATIE
CRISIS-OVERLEG







da's Willebroek
NOODPLANNING

TIJDLIJN
ACTIES CYBER-AANVAL WILLEBROEK
25 tem 31/01/2020

LOPENDE ACTIES
INTERNE COMMUNICATIE
EXTERNE COMMUNICATIE
CRISIS-OVERLEG

Impact

- In kaart brengen impact gebieden
  - Welke diensten, welke producten
  - Door afdelingshoofden
  - Kritieke zaken / prioriteiten
    - Gegevens rustoord bewoners (medicatie) + voorraadbeheer
    - Betalingen (lonen – leeflonen – budgetbegeleiding - externe leveranciers)
- Dienst-overschrijdende werkcellen :
  - continuïteit (van de dienstverlening)
  - (interne en externe) communicatie
  - ICT (remediëring en onderzoek)
  - Financiën
- Diensten
  - De diensten bleken in belangrijke mate zelfredzaam te zijn met betrekking tot hun regulier takenpakket.
  - Gebruik stand-alone laptops met 4G.
  - Gebruik stand-alone printer
  - Gebruik netwerk politie voor toegang Rijksregister
  - Gebruik typmachine

da's Willebroek

Impact

- Meldingsplicht

Hoewel initieel werd rekening gehouden met gegevensdiefstal leverde het onderzoek door ICT, SECUTEC en CCU vrij snel zekerheid dat er geen gegevens gestolen waren. Dit bleek oa uit een zorgvuldige screening van de log-files en werd finaal ook als dusdanig geattesteerd door SECUTEC.

Desalniettemin werd (pro-actief) aangifte gedaan bij:

- **Vlaamse Toezichtcommissie** (melding via CCVO – CrisisCentrum vd Vlaamse Overheid) (25/01)
- **GBA** (GegevensBeschermingsAutoriteit) (26/01)

Beide aangiften gebeurde ruim binnen de opgelegde termijnen en werden gelogd in ICMS.

De Privacy-commissie laat nadien in volle corona-crisis nog een specifieke externe audit uitvoeren bij ons bestuur.

da's Willebroek

Impact op de mensen

- Personeel
- Klanten
- Inwoners

da's Willebroek

NOODPLANNING
Mechelen - Willebroek

CYBER-AANVAL WILLEBROEK

GEMEENTELIJKE FASE

GEMEENTELIJK COÖRDINATIECOMITÉ

CRISIS-OVERLEG MANAGEMENTTEAM

COÖRDINATIE

4 CRISIS-CELLEN

CONTINUÏTEIT
CRISISWERKING / OPERATIONELE WERKING

COMMUNICATIE
INTERN / EXTERN

ICT
REMEDIËRING / GERECHTELIJK ONDERZOEK

FINANCIËN
BETALINGEN / STOCKBEHEER

EERSTE ACTIES

instructie-fiches bezoekers / gasten
instructie-fiches leidinggevenden
stand-alone IT-infrastructuur
FAQ-lijsten (intern / extern)
instructie-fiches personeel
flexibele personeelsinzet
crisis – werkprocessen
infolijn / mailadres
infovergaderingen

organisatie
WILLEBROEK

- 27.000 inwoners
- 27,5 km²
- 550 personeelsleden
- 15 vestigingen
- ca 200 producten
- 30.000 klantcontacten/jaar

IMPACT-CLUSTERS

SOCIAAL

woonzorgcentrum
thuiszorg
lokaal dienstencentrum
buitenschoolse opvang
kinderdagverblijf
OCMW
sociale diensten
...

DIENSTEN

onthaal
burgerzaken
technische diensten
openbare werken
ruimtelijke ordening
vergunningen
omgevingsloket
...

VRIJE TIJD

cultuur
sporthallen
evenementen
bibliotheek
...

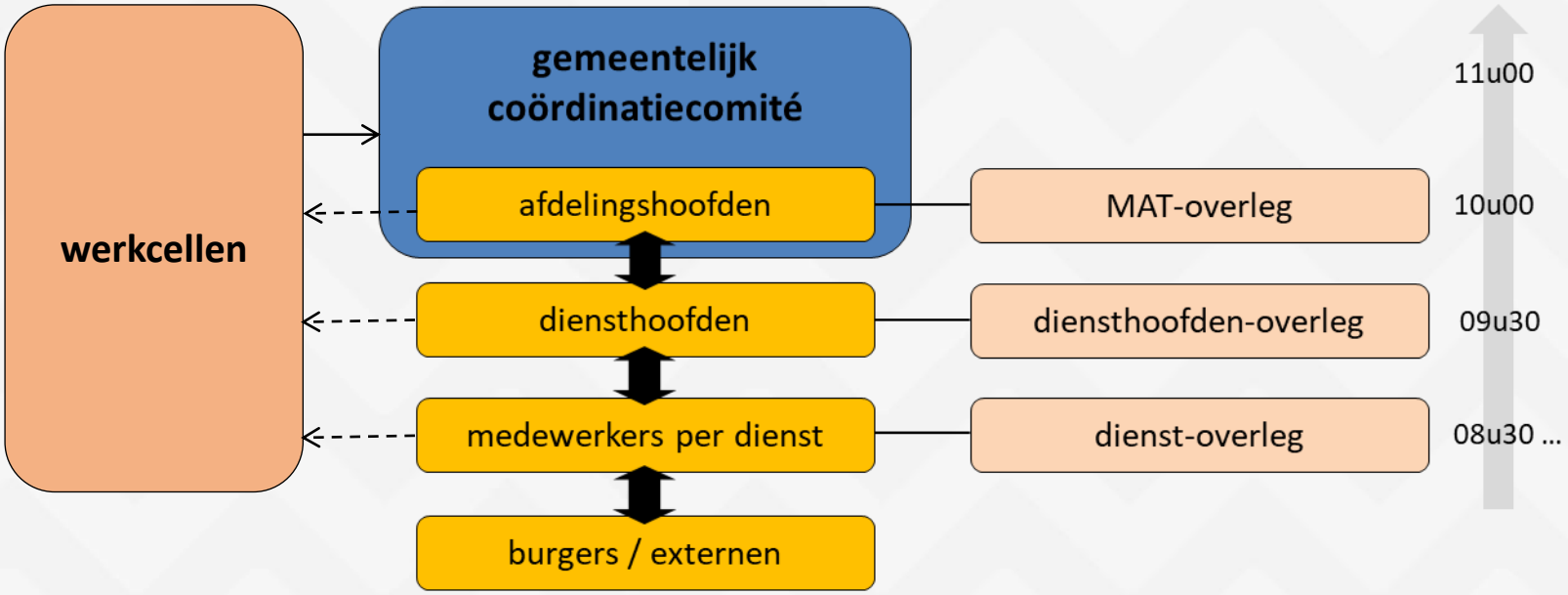
EXTERNEN

CAW
VDAB
CVO
...

da's Willebroek

Crisisbeheer

- Crisisbeheerstructuur



Crisisbeheer

- Geënt op de gekende crisisbeheersstructuren / -methodieken
  - Opschaling naar gemeentelijke fase
  - Multidisciplinaire aanpak
  - Monodisciplinaire opschaling
  - Vergaderstructuur en beeldvorming
- Duidelijke overlegstructuur
  - Gemeentelijk coördinatiecomité
  - Back-office en werkcellen
  - Terugkoppeling naar bovenlokale diensten/overheden
  - Terugkoppeling en aftoetsing binnen de eigen organisatie
  - Periodieke externe communicatie

da's Willebroek

Crisisbeheer

- Gemeentelijke crisiscel

Alle reguliere crisis-actoren werden betrokken:

- **D1** brandweerzone Rivierenland (BWZR) - postoverste Willebroek
- **D2** FOD Volksgezondheid - FGI/adj. FGI
- **D3** PZ Mechelen-Willebroek (MeWi) - korpschef / CP / LCCU
- **D4** Civiele Bescherming / grondgebiedszaken - OVD / afdelingshfd. grondgebiedszaken
- **D5** Communicatiedienst Willebroek - communicatieambtenaar
- **Burgemeester** + kabinetsmedewerkster
- **Noodplanningscoördinato**r + adj. NPC
- **FDG Antwerpen** DNP

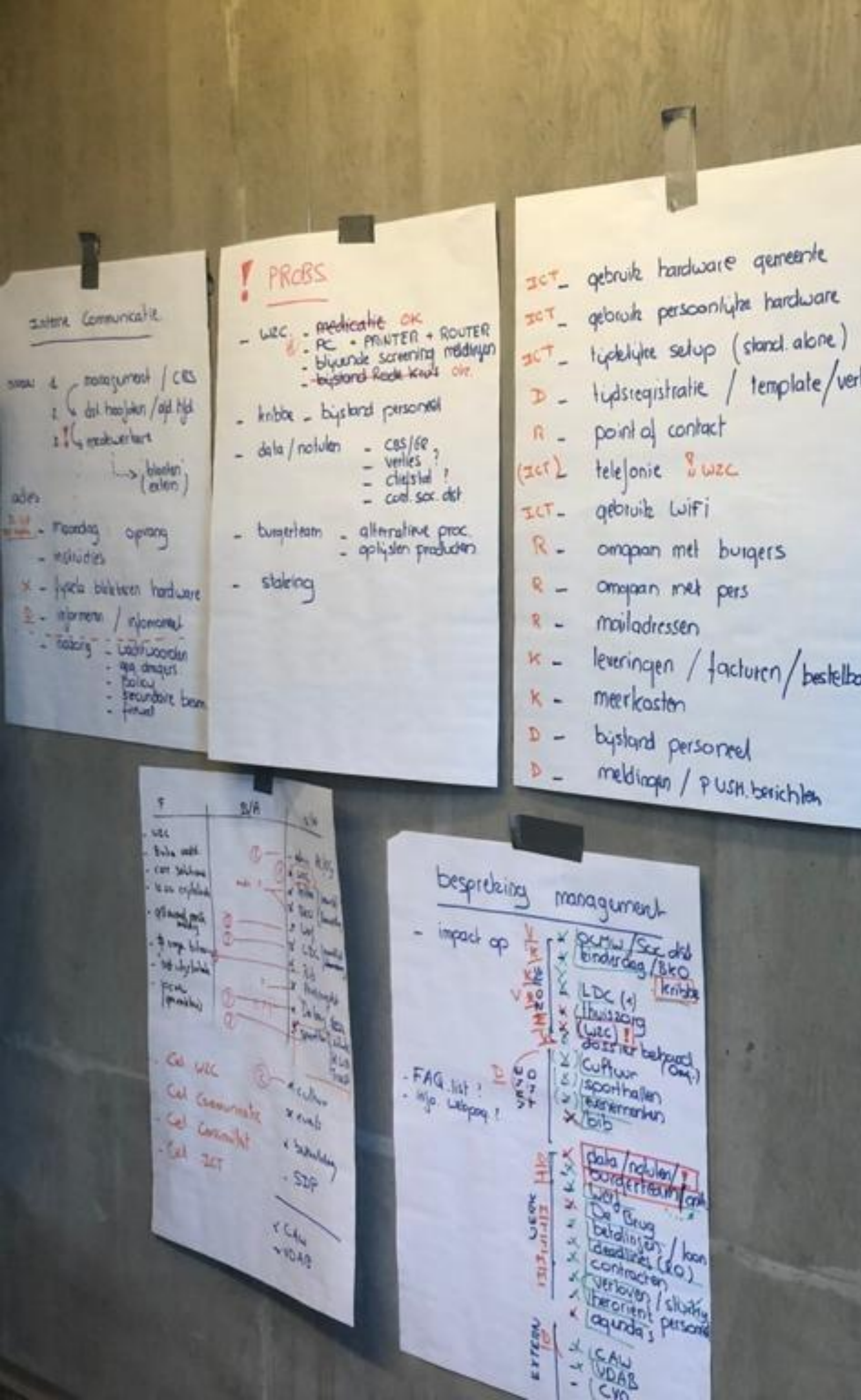
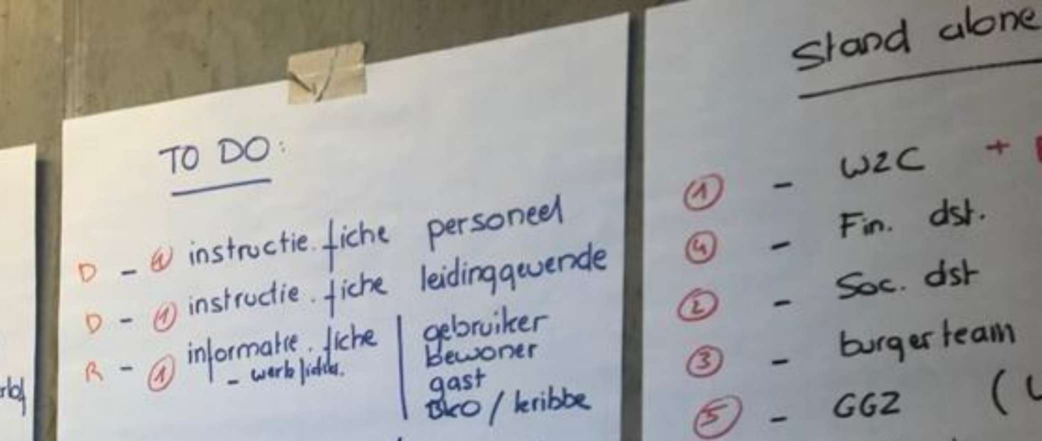
Aangevuld met:

- **Algemeen Directeur**
- **Experten**: ICT-dienst
- **Instelling**: directie WZC
- **Managementteam** (MAT) / afdelingshoofden

da's Willebroek

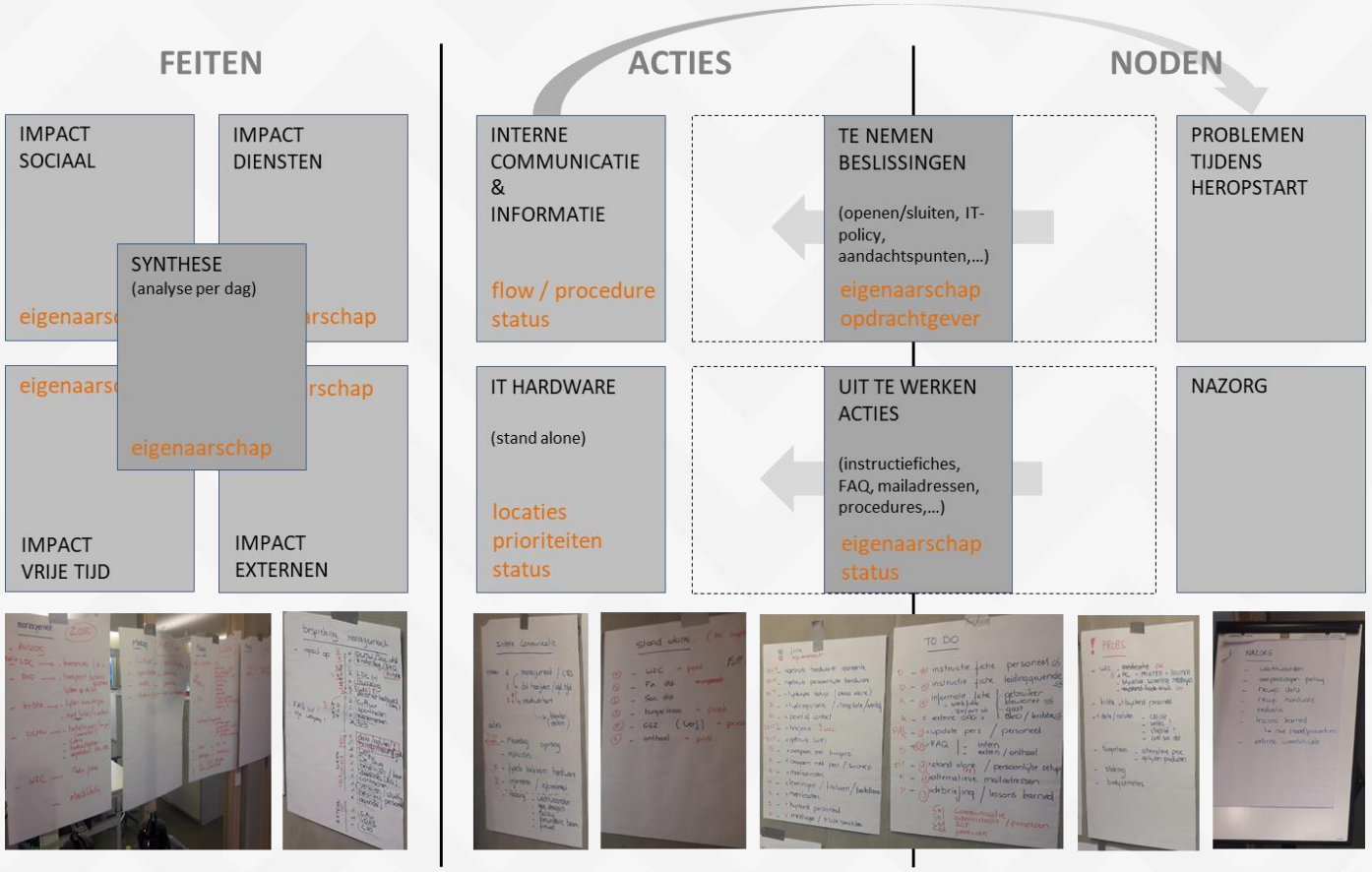
Gemeentelijke crisiscel (pré-corona tijdperk)

da's Willebroek



TO DO:
instructie fiche personeel
instructie fiche leidinggevende
informatie fiche
gebruiker
bewoner
gast
BKO / kribbe
stand alone
WZC
Fin. dst.
Soc. dst
burgerteam
GGZ
gebruik hardware gemeente
gebruik persoonlijke hardware
tijdelijke setup (stand alone)
tijdsregistratie / template / verlof
point of contact
telefonie
gebruik WiFi
omgaan met burgers
omgaan met pers
mailadressen
leveringen / facturen / bestelbon
meerkosten
bijstand personeel
meldingen / push berichten
bespreking management

Crisisbeheer

- Methodiek



Communicatie

- Er werd vanaf het begin van de crisis gekozen voor een zeer open en eerlijke communicatie naar het grote publiek.
  - Binnen crisis-communicatie staat deze strategie bekend als “stealing thunder”; een beproefde strategie die eruit bestaat als organisatie zo snel mogelijk slecht nieuws naar buiten te brengen in een poging maximaal controle te houden over de publieke perceptie.
- Eigen medewerkers op de hoogte brengen, los van berichtgeving in pers
  - 70% mondeling op de hoogte voor maandagochtend
  - Briefing op papier voor iedere medewerker bij aankomst op werkplek
    - Infofiche (wat wel – wat niet – wat te doen in geval van)
- Burgers
  - Info via website, sociale media, persberichten
  - Gratis infolijn
- Rusthuisbewoners en bezoekers
  - Aparte bewonersbrief met alle informatie
- Alternatieve mailadressen werden aangemaakt voor diverse diensten

da’s Willebroek

da's Willebroek

Instructiefiches voor de leidinggevende

ACTIES TE NEMEN BINNEN JE DIENST:

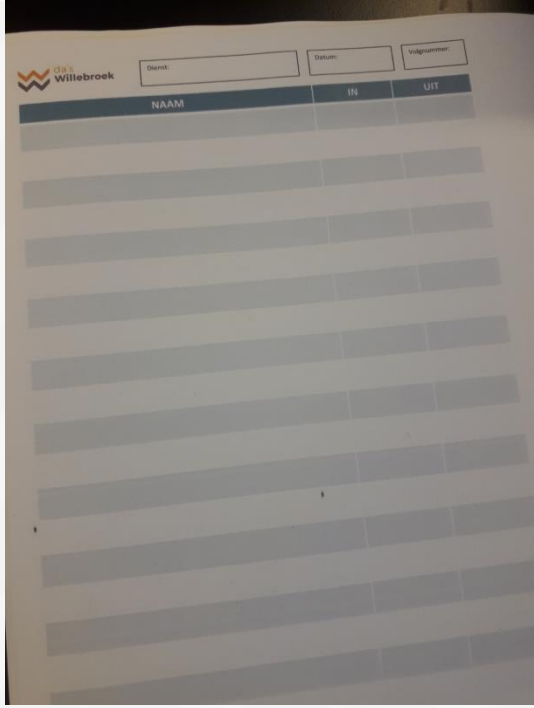
ONTHAAL PERSONEEL
- ❑ plaats een medewerker aan alle ingangen
- ❑ zorg dat al je medewerkers bij binnenkomst een instructiefiche krijgen
- ❑ volg op dat alle medewerkers in-/uittikken én de IN/OUT-lijst invullen
- ❑ controleer dat medewerkers geen eigen laptop/tablet meebrengen
- ❑ verzamel dienst-laptops/-tablets

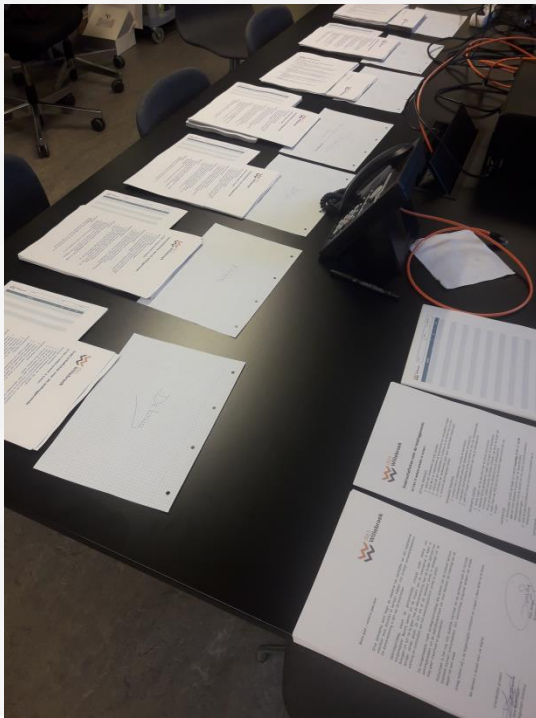
INFORMATIE PERSONEEL
- ❑ overloop met je medewerkers in groep de beschikbare informatie/instructies zodra alle medewerkers aanwezig zijn
- ❑ organiseer informatiedeling binnen je dienst (bv dmv een Whatsappgroep)
- ❑ geef ICT-vragen van medewerkers door naar je afdelingshoofd

INFORMATIE DERDEN
- ❑ verwijs vragen van de pers door naar de dienst communicatie
- ❑ behandel dienst-gerelateerde vragen van burgers ifv de beschikbare informatie; indien concrete vragen ontbreekt: zeg dat je de burger zelf terug zal contacteren na aftoetsing met je afdelingshoofd
- ❑ maak intern een FAQ-lijst op met courante vragen/antwoorden van burgers

RAPPORTAGE
- ❑ diensthoofden worden gevraagd om uiterlijk **maandag 27/01** om **10.00 uur** een korte feedback te geven naar de respectievelijke afdelingshoofden rond de opstart van hun dienst (eventuele problemen, personeelsvragen,...)
- ❑ meld dringende problemen binnen je dienst onmiddellijk aan je afdelingshoofd

INFOMOMENT
- ❑ **maandag 27/01** om **14.00 uur** zal een kort infomoment voor de diensthoofden georganiseerd worden in de oude lokettenzaal





Recovery

- Check backups
- Start eerste restores zondagavond
  - Prioriteit voor woonzorgcentrum – om dit zo snel mogelijk operationeel te hebben
  - Woonzorgcentrum operationeel maandagmorgen
- Maandag verdere restore andere servers (25)
- Dinsdagochtend 11u alles terug operationeel van backup
  - Rest van de dag worden door diensten hun applicaties uitvoerig getest om na te gaan of alle functionaliteiten beschikbaar waren.
  - Aantal koppelingen met externe overheden en sommige leveranciers werd hersteld
- Recentste versie anti-virus werd uitgerold

da's Willebroek

Recovery/aanbevelingen

- Zorg voor regelmatige patching/firmware updates van je cruciale componenten
- Zorg voor actuele en veilige backup
- Test regelmatig restore van je backup
- Indien financieel mogelijk, zorg voor een off-line backup
- Informeer je medewerkers over potentiële gevaren
- Strenge password policy kan helpen
- Zorg voor een up-to-date anti-virus
- …maar denk er aan, je bent nooit 100% beveiligd!

da's Willebroek

Innerlijke mens

da's Willebroek

Wat hebben we geleerd?

Roxane Kerssebeeck van de gemeente Willebroek is aangewezen op een typmachine na een computerhack © David Legreve

Gemeente Willebroek gaat creatief aan het werk na cyberaanval: "Dit is de beste teambuilding ooit"

da's Willebroek

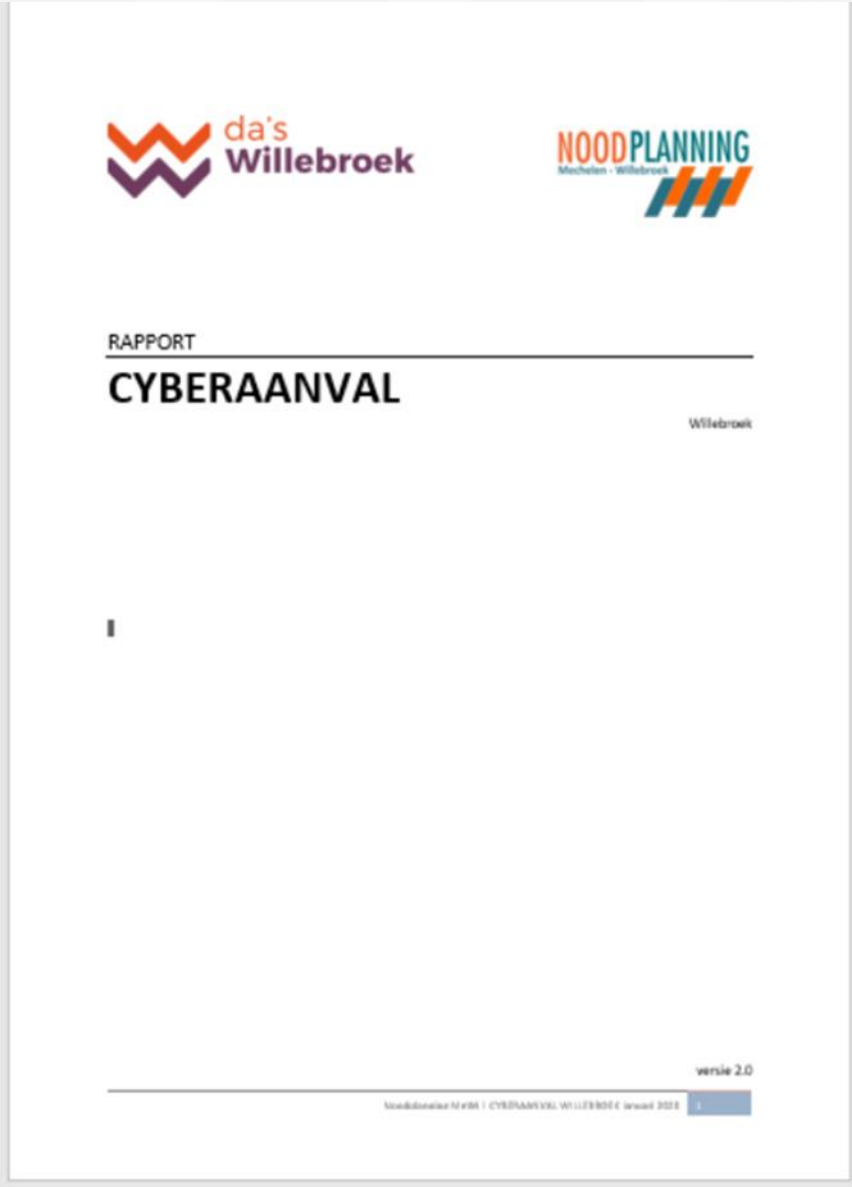
Rapport

Tips & tricks

Op te vragen bij:

Dirk Blommaert via

dirk.blommaert@willebroek.be



Vragen?

Van harte dank.

da's Willebroek