

KEUZEMODULE *CYBERSECURITY* WEERBAAR TEGEN CYBERCRIME

Module 1 - Wat is cybersecurity en cybercrime?

Workshop 2 - Risicodenken en -management



LEERUITKOMST MODULE 1

Je hebt een fundamenteel begrip van cybersecurity en bent met een risico-bewuste mentaliteit in staat om wet- en regelgeving, risicomanagement en het beheer van cybersecurity toe te passen in een organisatie, zodanig dat daarmee effectief wordt bijgedragen aan het beveiligingsbeleid en risicobeheer binnen organisaties.

Overzicht

Week 1: Risicodenken

- Workshop 1: De wereld van cybercrime
- Workshop 2: Risicodenken en -management
- Workshop 3: Governance van cybersecurity

Week 2: Risicoanalyse

- Workshop 4: Risico-assessment
- Workshop 5: Beveiligingsmaatregelen

Week 3: Challenge, uitstapje en afronding

WAT HEBBEN WE TOT NU TOE GEDAAN?

De wereld van cybercrime

In de vorige workshop hebben we ontdekt welke vormen van cybercrime er zijn, wie (welk soort criminelen) zich er mee bezig houden en wie slachtoffer kunnen worden. We weten nu waarom cybersecurity zo belangrijk is.

WAARMEE GA JE VANDAAG AAN DE SLAG?

Leeruitkomst workshop

- Je hebt begrip bij wat een risico is en hoe je hier mee omgaat in de verschillende stadia waarin risico's voor kunnen komen. De kennis over risicobehandeling kun je – in de basis – vertalen naar concrete maatregelen.
- Je bent vertrouwd met de wet- en regelgeving en normen die relevant zijn voor cybersecurity. Je begrijpt de vereisten waaraan organisaties moeten voldoen om een effectieve cybersecuritystrategie te ontwikkelen en implementeren.

AGENDA WORKSHOP 2

- Risico
- Risicobehandeling
- Incident- en beveiligingscyclus

- Opdracht
- Tips voor bronnen

WAT IS EEN RISICO?

Risico (in relatie tot cybersecurity) is de kans dat een potentieel gevaar resulteert in een daadwerkelijk incident en wat het gevolg hiervan is voor de bedrijfsvoering van een organisatie.

In formulevorm: **Risico = Blootstelling * Kans * Gevolg**

Blootstelling (B) = wanneer en waar het gevaar zich voordoet

Kans (waarschijnlijkheid, W) = de waarschijnlijkheid dat de gevolgen optreden naar aanleiding van de blootstelling

Gevolg (effect, E) = het effect of de consequentie van het optreden van een incident

$R = B * W * E$ (Kinney en Wiruth)

RISICO'S PRIORITEREN

Blootstelling		
0,5	Zeer Zelden	1 keer per jaar of minder
1	Zelden	Enkele keren per jaar
2	Uitzonderlijk	1 keer per maand
3	Af en toe	1 keer per week
6	Regelmatig	1 keer per dag
10	Voortdurend	permanent

Kans		
0,1	Bijna niet denkbaar	1 op 1.000.000
0,2	Praktisch onmogelijk	1 op 100.000
0,5	Denkbaar maar zeer onwaarschijnlijk	1 op 10.000
1	Mogelijk, is al wel eens gebeurd	1 op 1.000
3	Ongewoon, maar mogelijk	1 op 100
6	Kan zich voordoen	1 op 10
10	Kan verwacht worden	1 op 1

[Video: Risk and How to use a Risk Matrix](#)

Gevolg					
	Omschrijving	Kosten	Imago	Continuïteit	Letsel
1	Weinig significant	100	Geen	Geen invloed	Ehbo
3	Belangrijk	1.000	Gering	Halve dag	Licht
7	Zwaar	10.000	Enige	Hele dag	Zwaar
15	Zeer zwaar	100.000	Redelijk	2 dagen	Blijvend letsel
40	Ramp	1.000.000	Aanzienlijk	1 week	Dode
100	Catastrofe	10.000.000	Zeer groot	2 weken	Vele doden

Tabel met getalswaarde van het risico bij een activiteit

Invoer: kans en effect

Uitkomst: getalswaarde van risico met risico-niveau in kleur

groen:	laag risico
geel	gemiddeld risico
rood	hoog risico

		kans				
zeer onwaarschijnlijk 1	onwaarschijnlijk 2	mogelijk 3	kansrijk 4	zeer kansrijk 5		
Het risico heeft zich voor zover bekend nog niet voorgedaan in de branche/bedrijfstak.	Het risico heeft zich voorgedaan in de branche/bedrijfstak.	Het risico heeft zich voorgedaan in vergelijkbare omstandigheden	Het risico doet zich verschillende keren per jaar voor.	Bijna zeker dat het risico zich zal voordoen.		
De activiteit vindt zelden plaats.	De activiteit vindt af en toe plaats.	De activiteit vindt regelmatig plaats.	De activiteit vindt vaak plaats.	De activiteit wordt continu uitgevoerd.		
		effect				
		mensen	milieu	materieel		
minimaal	1	EHBO noodzakelijk. Geen onderbreking van werkzaamheden.	schade < €500	Minimale plaatselijke schade	laag (1)	laag (2)
matig	2	Minimale gezondheidseffecten. Geen verzuimdagen.	schade < €5.000	Lichte schade die met minimale kosten ter plaatse gerepareerd kan worden.	laag (2)	laag (4)
ernstig	3	Gezondheidseffecten die echter nog wel te genezen/te verhelpen zijn. Met verzuimdagen.	schade < €50.000	Matige schade die gerepareerd kan worden met niet al te hoge kosten.	laag (3)	gemiddeld (6)
groot	4	Blijvend letsel en/of levensbedreigende verwondingen met veel verzuimdagen en er kan zelfs een dode bij betrokken zijn.	schade < €100.000	Grote schade die met hoge kosten gerepareerd kan worden en met eventuele juridische gevolgen.	laag (4)	gemiddeld (8)
catastrofaal	5	Een aantal doden.	schade ≥ €100.000	Zware schade over een lange periode, kan leiden tot (tijdelijke) buiten gebruikstelling/evacuatie, lokale betrokkenheid, juridische gevolgen.	gemiddeld (5)	gemiddeld (10)
					hoog (15)	hoog (20)
					hoog (20)	hoog (25)

RISICOBENADERING EN SCENARIOBENADERING

Risicobenadering =

zet de risico's in volgorde van groot naar klein. De risico's die groot zijn, verklein je met het nemen van maatregelen tot een acceptabel niveau. Zo richt je inspanningen op risico's waar de meeste veiligheidswinst te behalen valt.

Scenariobenadering =

Je gaat er vanuit dat het misgaat. Je maakt een scenario over het incident. Zo zorg je dat je voorbereid bent als het misgaat. Je treft bij scenariobenadering vooral preparatie- en repressiemaatregelen. De scenariobenadering gaat uit van de gevolgen van een risico.

RISICOBEHANDELING (MANAGEMENTSTRATEGIEËN)

Avoid

Eliminate the risk by avoiding the activity or situation that caused it.

Transfer (share)

Pass the risk to another party, such as through insurance or outsourcing.

Mitigate

Implement controls or actions to reduce the likelihood or impact of the risk.

Accept

Acknowledge the risk and its consequences, and prepare to manage the outcome.

(Share) Split the risk between multiple parties

Voorbeelden?

BETROUWBAARHEID VAN INFORMATIEVOORZIENING (DIE WIL JE GARANDEREN!)

Beschikbaarheid

Availability

Integriteit

Integrity

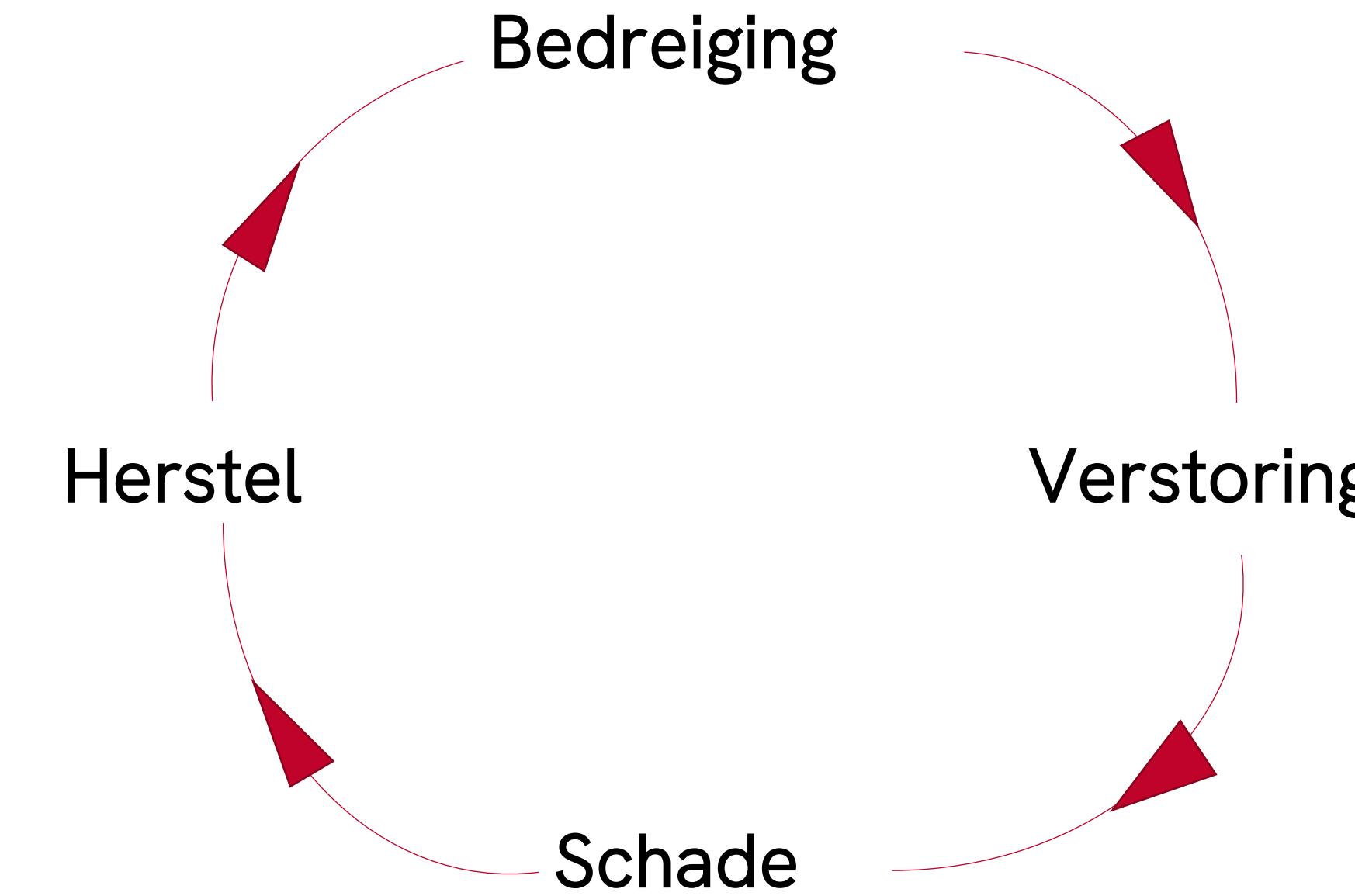
Vertrouwelijkheid

Conidentiality

BIV

CIA

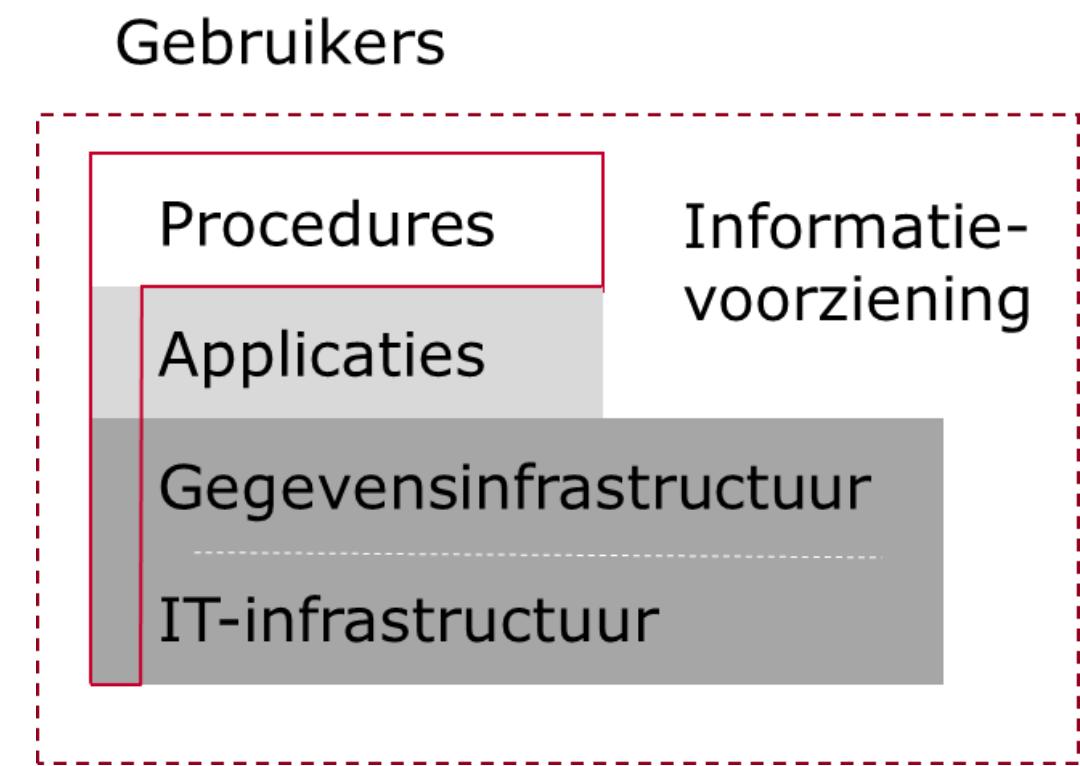
MAAR... GEVAREN LIGGEN OP DE LOER: DE INCIDENTCYCLUS



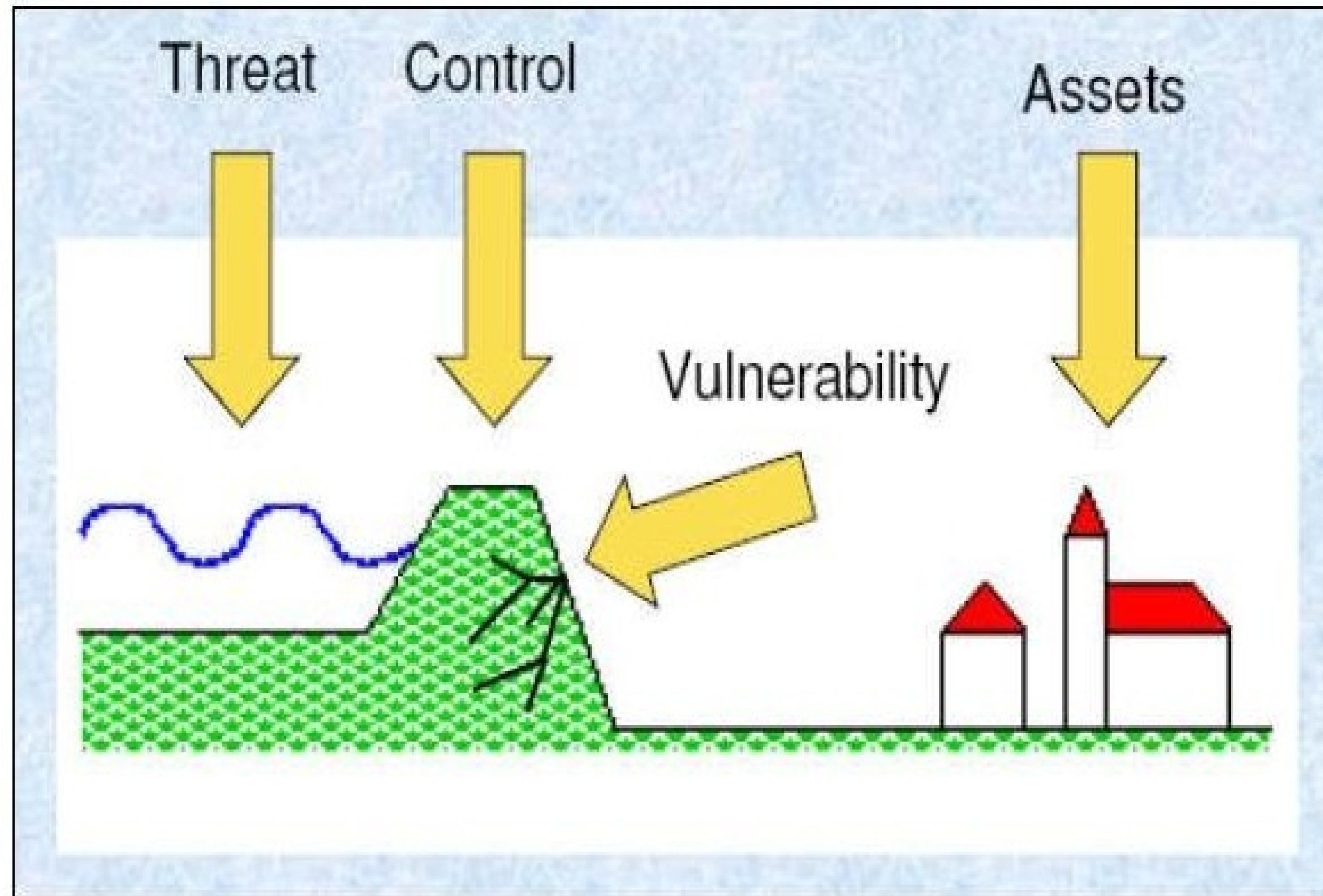
- Bedreiging: iets dat zou kunnen gebeuren (bv. hackers, stroomstoring)
- Verstoring: Als de bedreiging leidt tot een incident
- Schade: Door een incident kan schade ontstaan aan informatie of middelen
- Herstel: Het herstellen van de ontstane schade

DREIGING, GEVAAR

- Een dreiging is een proces of gebeurtenis die in potentie een verstorende invloed heeft op een **object** van de informatievoorziening: Apparatuur, programmatuur, gegevens, procedures, mensen
- De dreiging kan zowel van buiten (hacker) als van binnen (frauderende medewerker) komen.
- Als de dreiging werkelijkheid wordt, dan resulteert dat in schade aan belangen: assets → waardevolle eigendommen, het openbaren van informatie en/of verstoring van waardevolle processen.
- Een dreiging wordt pas relevant als sprake is van een **kwetsbaarheid** voor een belang (asset) en een kwaadwillende die de **intentie** heeft om het belang aan te vallen.



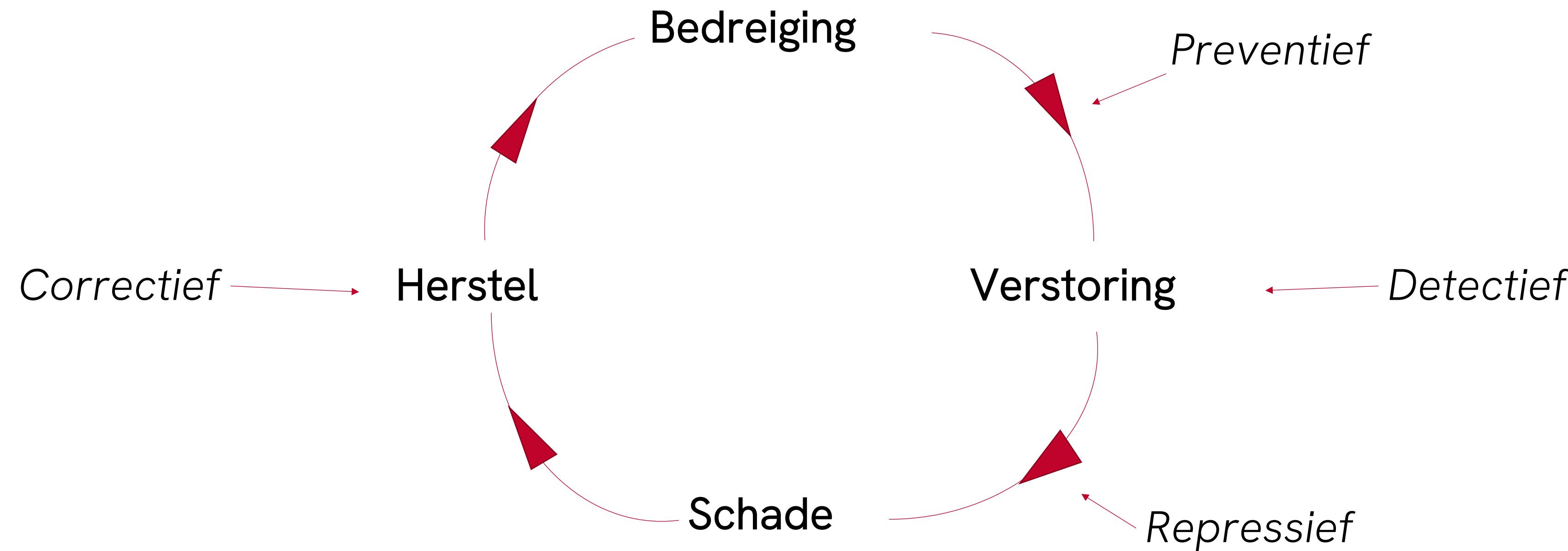
NET ALLEEN KWAADWILLENDEN



- Wateroverlast
- Kabelbreuk
- Brand
- Softwarefout
- Stroomstoring
- ...

DE BEVEILIGINGSCYCLUS

MAATREGELEN NEMEN OM DE BETROUWBAARHEID TE VERGROTE

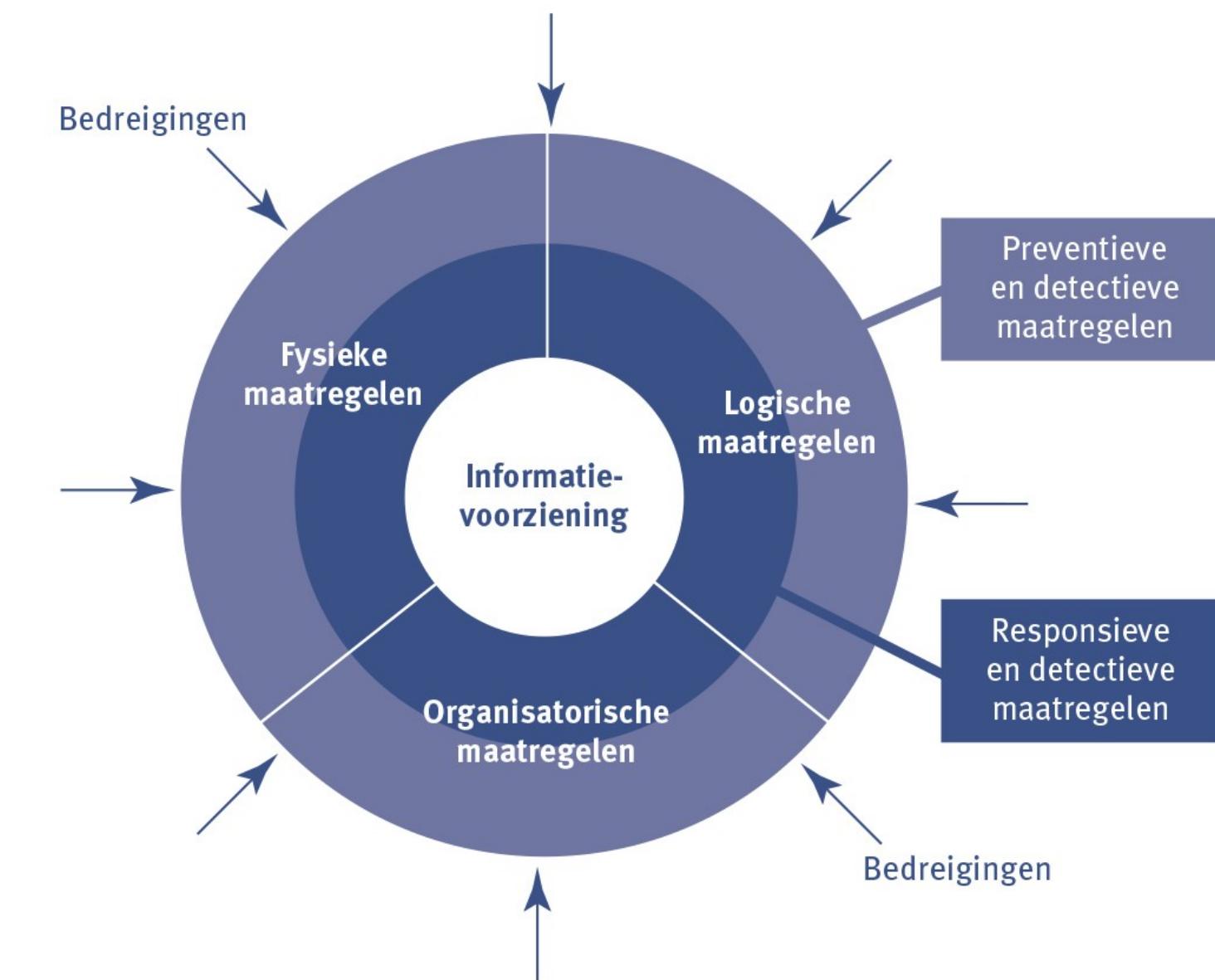


- Preventief: Voorkomen dat bedreigingen tot een verstoring leiden
- Detectief: Een incident zo snel mogelijk ontdekken. Ondersteunend voor preventie en repressie
- Repressief: De negatieve invloed van een verstoring minimaliseren
- |15 • Correctief: Herstellen van objecten die bij een incident beschadigd zijn

MAATREGELEN

- Organisatorische maatregelen
 - Hebben betrekking op organisatie, mensen, procedures
- Logische maatregelen
 - Zijn opgenomen in de programmatuur (applicaties /software)
- Fysieke maatregelen
 - Zijn gerealiseerd met apparatuur of andere materiële middelen

dd/mm/jjjj



FIGUUR 2.9

Beveiligingsmaatregelen schematisch ingedeeld naar hun plaats in de beveiligingscyclus en de wijze waarop ze gerealiseerd worden

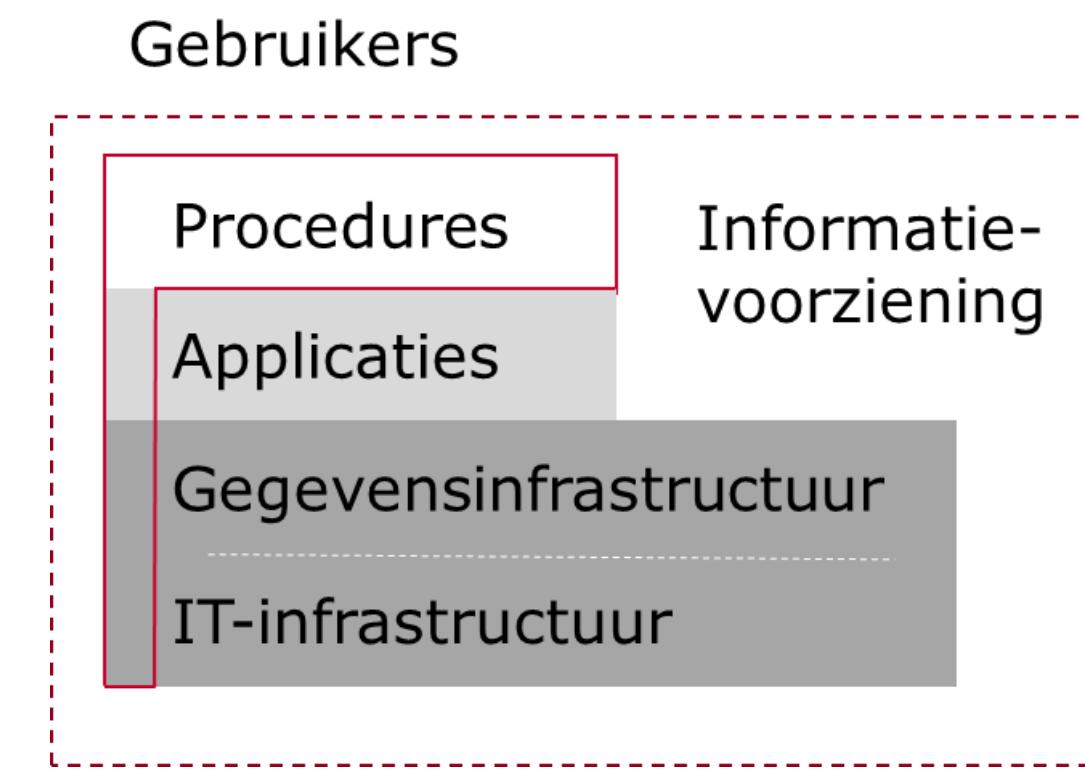


VOORBEELDEN

TYPES OF SECURITY CONTROLS	CONTROL FUNCTIONS		
	PREVENTATIVE	DETECTIVE	CORRECTIVE
	PHYSICAL CONTROLS <ul style="list-style-type: none"> • Fences • Gates • Locks 	<ul style="list-style-type: none"> • CCTV • Surveillance Cameras 	<ul style="list-style-type: none"> • Repair physical damage • Re-issue access cards
	TECHNICAL CONTROLS <ul style="list-style-type: none"> • Firewall • IPS • MFA • Antivirus 	<ul style="list-style-type: none"> • IDS • Honeypots 	<ul style="list-style-type: none"> • Vulnerability patching • Reboot a system • Quarantine a virus
ADMINISTRATIVE CONTROLS	<ul style="list-style-type: none"> • Hiring & termination policies • Separation of duties • Data classification 	<ul style="list-style-type: none"> • Review access rights • Audit logs and unauthorized changes 	<ul style="list-style-type: none"> • Implement a business continuity plan • Have an incident response plan

VERSCHILLENDENDE KIJK OP MAATREGELEN

- Naar de plaats in de beveiligingscyclus
 - Preventief
 - Detectief
 - Repressief
 - Correctief
 - Naar de wijze waarop ze gerealiseerd worden
 - Organisatorisch
 - Logisch
 - Fysiek
 - Naar het aspect van de betrouwbaarheid van de informatievoorziening dat ze beveiligen:
 - Beschikbaarheid
 - Integriteit
 - Vertrouwelijkheid
- 1 maatregel kan meer dan één aspect tegelijkertijd beveiligen



GROEPSOPDRACHT: WETGEVING EN NORMEN

Doel: Je vertrouwd maken met de **wet- en regelgeving** en **normen** die relevant zijn voor cybersecurity. Door onderzoek te doen naar deze richtlijnen ga je de vereisten begrijpen waaraan organisaties moeten voldoen om een effectieve cybersecuritystrategie te ontwikkelen en implementeren.

Ga als volgt te werk:

1. Onderzoek de wet- en regelgeving en normen die van kracht zijn rond cybersecurity, zowel op nationaal als internationaal niveau. Ieder groepslid kiest hierbij één norm of wet.
2. Focus op relevante wetten, regelgevingen en normen, zoals, maar niet uitsluitend: AVG (GDPR), ISO27001, NIST Cybersecurity Framework, NIS2 maar bijvoorbeeld ook de wet Computercriminaliteit III.
3. Gebruik verschillende bronnen, waaronder overheidswebsites, officiële publicaties, en betrouwbare organisaties op het gebied van cybersecurity.
4. Beantwoord de volgende vragen als **leidraad** voor jullie onderzoek:
 1. Welke nationale en internationale **wetten** zijn van toepassing op cybersecurity?
 2. Wat zijn de belangrijkste vereisten van deze wetten en regelgevingen met betrekking tot cybersecurity?
 3. Welke **normen** worden vaak gebruikt als referentie voor best practices in cybersecurity? Op welke sectoren zijn ze van toepassing?
 4. Hoe worden deze normen toegepast in de praktijk binnen organisaties?
 5. Wat zijn de voordelen voor organisaties om te voldoen aan deze wetten, regelgevingen en normen?
 6. Wat zijn de recente ontwikkelingen of updates in wet- en regelgeving die van invloed zijn op cybersecurity?
5. Verwerk de resultaten in een matrix waarin de verschillende wetten, regelgevingen en normen worden vermeld met hun belangrijkste vereisten en toepassingsgebieden (sectoren, soort organisaties).
6. Een aantal groepen zal hun uitkomsten vanmiddag presenteren in min. 5 en max. 10 minuten voor de klas.

BRONNEN

- Zie Bibliotheek op Brightspace en.. Internet!

BEGELEIDING

- Vanmiddag consultatie in workshop van 14.00 uur.
- Morgenochtend mogelijkheid om online met docenten te schakelen tussen 9.00 en 11.30 uur.