THE CYBER PARTNERS
de 'booking.com' van cyber

CYRA CYBER RATING

IQ Tech Event

workshop:
"cybersecurity in focus"

door Evelien Bras
06 maart 2025

Read More

Evelien Bras:

- commissaris / board advisor
- gastdocent “Corporate Governance”
- DGA The Cyber Partners B.V.
- voorzitter bestuur “CYRA: Cyber-Rating”
- commissie van belanghebbenden CCV
- penvoerder “Cyberweerbaarheidscentrum Oost Nederland”

Aangenaam kennis te maken.

THE CYBER PARTNERS

Rechter: Hof van Twente zelf schuldig aan hack

15 MEI 2023 - 10:10 | 5 MINUTEN LEESTIJD | ACTUEEL | GOVERNANCE & PRIVACY | DUSTIN

Rik Sanders

De gemeente Hof van Twente, op 1 december 2020 slachtoffer van een hack die de it-systemen lamlegde, eiste vier miljoen schadevergoeding van partner Switch IT Solutions wegens wanpresteren. De rechtbank in Almelo oordeelt echter dat de it-dienstverlener uit Enschede, onderdeel van het Zweedse Dustin, geen blaam treft. Hof van Twente is zelf verantwoordelijk voor het incident door een lakse houding.

Eind 2020 kwam een stroom losgeldbrieven uit vijftig printers in het gemeentehuis in Goor. De hackers waren de baas over het gemeentelijke netwerk en eisten 750.000 euro losgeld. De gemeente betaalde niet en de gevolgen waren groot. Systemen werden vernietigd en data versleuteld of gestolen. Uiteindelijk was de gemeente ruim vier miljoen euro

19:53
◂ Safari

AD

▲ Foto ter illustratie. © Thinkstock

Criminelen plaatsen 'gevoelige' gegevens van Arnhemmers op dark web na cyberaanval

Lars Barendregt
26 februari 2025, 16:59 • **update: 26 februari 2025, 18:45**

2:36 Artikel luisteren

Gevoelige persoonlijke gegevens van zeker tientallen Arnhemmers zijn gestolen door cybercriminelen. Dat zegt de gemeente. Mogelijk zijn ook inwoners van andere gemeenten slachtoffer. De criminelen pleegden midden januari een digitale aanval bij een van de ict-leveranciers van de gemeente Arnhem.

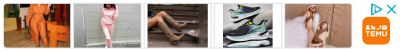
19:48

FANNI FORGÁCS / 3 MAART 2025 /

MAATSCHAPPIJ

Internationale hacktivistengroep lanceert driedaagse cyberaanval op Hongaarse websites, waaronder Daily News Hungary — BIJGEWERKT

Foto: depositphotos.com



dailynewshungary.com

19:50

Geen vervolg op losgeldeis

Cyberaanval op Zuid-Afrikaanse weerdienst blijft onopgemerkt

Een cyberaanval op de Zuid-Afrikaanse weerdienst op 26 januari 2025 door een organisatie met de naam RansomHub is nauwelijks opgemerkt door de AGF-sector. Geen enkele teler of teeltmanager die door FreshPublishers werd benaderd, wist dat de Zuid-Afrikaanse nationale weerdienst was gehackt.

De weerdienst kondigde de cyberaanval de volgende dag aan en merkte op dat het "de tweede in twee dagen tijd was nadat de eerste poging op zaterdag 25 januari 2025 was mislukt".

Gedurende de drie weken tussen 26 januari en 19 februari stond hun centrale computersysteem niet in contact met de satellietweerstations en de weersvoorspellingsmodellen waarop gebruikers vertrouwen voor nauwkeurige weersvoorspellingen, draaiden in feite op geëxtrapoleerde gegevens.

Er wordt gevreesd dat de klimaatgegevens die de weerdienst sinds het begin van de twintigste eeuw heeft verzameld, verloren kunnen gaan achter een ondoordringbare encryptie die is ingesteld door de hackers, die naar verluidt dreigden de gehackte gegevens op het dark web te publiceren.

De hackers gaven een losgeldbrief uit, maar, merkt Oupa Segalwe op, hoofd communicatie bij de Zuid-Afrikaanse weerdienst, "er was geen specificiteit met betrekking tot het losgeldbedrag. De hackers hebben ook geen vervolgacties ondernomen."

agf.nl

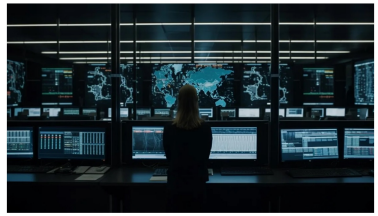
19:52

Dutch iT Channel

Cyberaanval op Orange Group

Orange Group is getroffen door een cyberaanval. Online is een grote hoeveelheid gegevens gepubliceerd die van klanten van Orange Group zouden zijn.

Security | Data protection



Een hacker beweert duizenden interne documenten met gebruikersgegevens en personeelsinformatie te hebben gestolen na een aanval op de systemen van Orange Group, een groot Frans telecom- en digitaal dienstverleningsbedrijf. De aanvaller, die zich online Rey noemt en lid is van de HellCat-ransomwaregroep, zegt dat de gestolen data voornamelijk afkomstig is van de Roemeense tak van het bedrijf en bestaat uit 380.000 unieke e-mailadressen, broncode, facturen, contracten en klant- en personeelsgegevens.

Data gepubliceerd

dutchitchannel.nl

Context:

- 3 op de 5 bedrijven verwacht een cyberaanval in 2025
- 76% van de IT-ers en CISO’s ervaart (te) veel stress en overweegt een andere baan
- 60% geeft aan dat er een gebrek aan strategische prioriteit is: multidisciplinaire aanpak: Techniek / Mensen / Processen
- Inhoudelijk gaan de ontwikkelingen snel, zeker na introductie van AI.

Workshop doelen:

- Cyber gaat gedreven worden vanuit wetgeving, compliancy, hoe kun je hier mee omgaan?
- Hoe stuur je een (externe) IT organisatie zonder detailkennis van techniek?
- Hoe stuur je uitvoer multidisciplinair aan?
- Sturen op standaardisatie bij implemenatie.

Twee richtlijnen/wetten uitgelicht:

- NIS-2
  Network Information Security
  Europese directive
  Cyberweerbaarheidswet

- CRA
  Cyber Resilience ACT
  European regulation

- Persbericht lezen aan de hand van het “Cyber Governance Model”

De NIS-2 is een Europese richtlijn

Voor organisaties van 50+ FTE
in een van 18 sectoren.

en omvat:
- meldplicht
- cyberrisicobeheersmaatregelen (zorgplicht) en
- rapportageverplichtingen

Naar schatting 8000 bedrijven in Nederland gaan onder de NIS-2 vallen, zijnde ‘essentieel’ of ‘belangrijk’.

Zelf controleren?
https://regelhulpenvoorbedrijven.nl/NIS-2-NL/

THE CYBER PARTNERS

Welke maatregelen moet ik nemen om aan de zorgplicht te voldoen?

Onder de zorgplicht vallen ten minste:

1. Een risicoanalyse en beveiliging van informatiesystemen
2. (Beleid en procedures over) incidentenbehandeling
3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen
4. Beveiliging van de toeleveranciersketen
5. Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden
6. Beleid en procedures om de effectiviteit van beheers-maatregelen van cyberbeveiligingsrisico's te beoordelen
7. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging
8. Beleid en procedures over het gebruik van cryptografie en encryptie
9. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa
10. Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde nood-communicatiesystemen binnen de entiteit

Bron: ncsc.nl
Stuur mail voor link naar samenwerkingsportal

THE CYBER PARTNERS

Regulation 2024/2847

Cyber Resilience Act (CRA)

De Cyber Resilience Act (CRA) is een Europese verordening die zich richt op het verbeteren van de beveiliging van digitale producten en diensten. De verordening is gepubiceerd en eind 2024 in werking getreden.

Omdat de CRA een verordening is, hoeft deze niet vertaald te worden naar Nederlandse wetgeving, maar is deze direct van kracht. Eind 2027 moeten vervolgens alle producten met digitale elementen als inherent veilig ontworpen en geproduceerd zijn (zogeheten security-by-design). Daarnaast geldt voor fabrikanten en andere partijen in de toeleveringsketen een zorgplicht, waaronder het aanbieden van ondersteuning en beveiligingsupdates en een meldplicht bij kwetsbaarheden en incidenten.

Welke producten moeten aan de CRA voldoen?

Alle producten met digitale elementen moeten vanaf 2027 voldoen aan de CRA. Dit zijn niet alleen fysieke producten zoals IoT-apparatuur, firewalls of netwerkapparatuur, maar ook software zoals videogames, mobiele apps of besturingssystemen zoals Windows en componenten zoals videokaarten en software libraries.

THE CYBER PARTNERS

- Werk **risicogebaseerd** aan cyber-volwassenheid, ook voor de NIS-2.

- Leg verantwoordelijkheden op de juiste plek. **Bestuur / uitvoer**

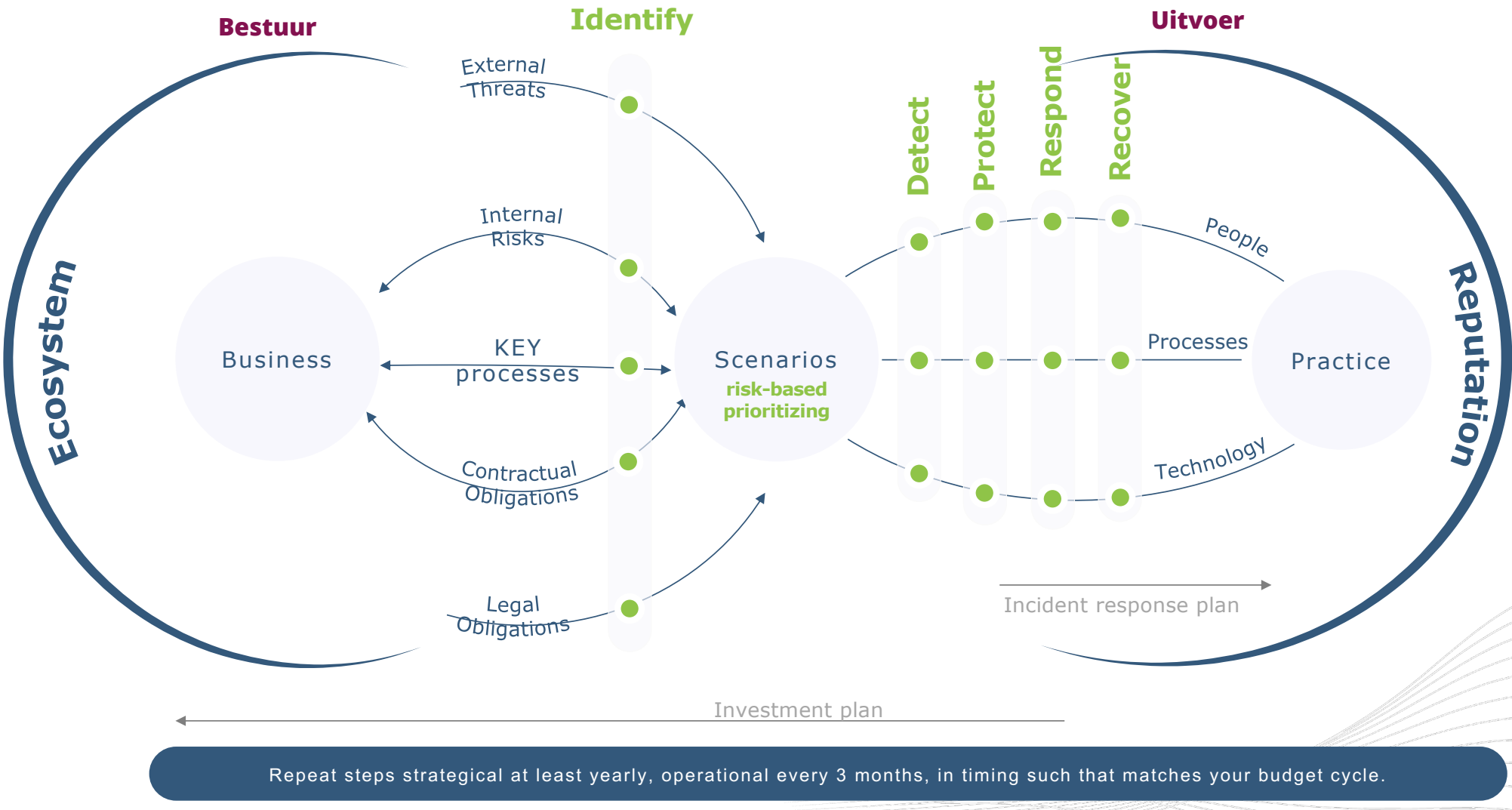
- Bevraag in een vroeg stadium je klanten voor (standaard in) **aantoonbaarheid.**

- Betrek **legal en inkoop,** vooruitlopend op de CRA, het kan je een voorsprong geven.

- Hou het CCV (hetccv.nl) in de gaten voor standaardisatie.

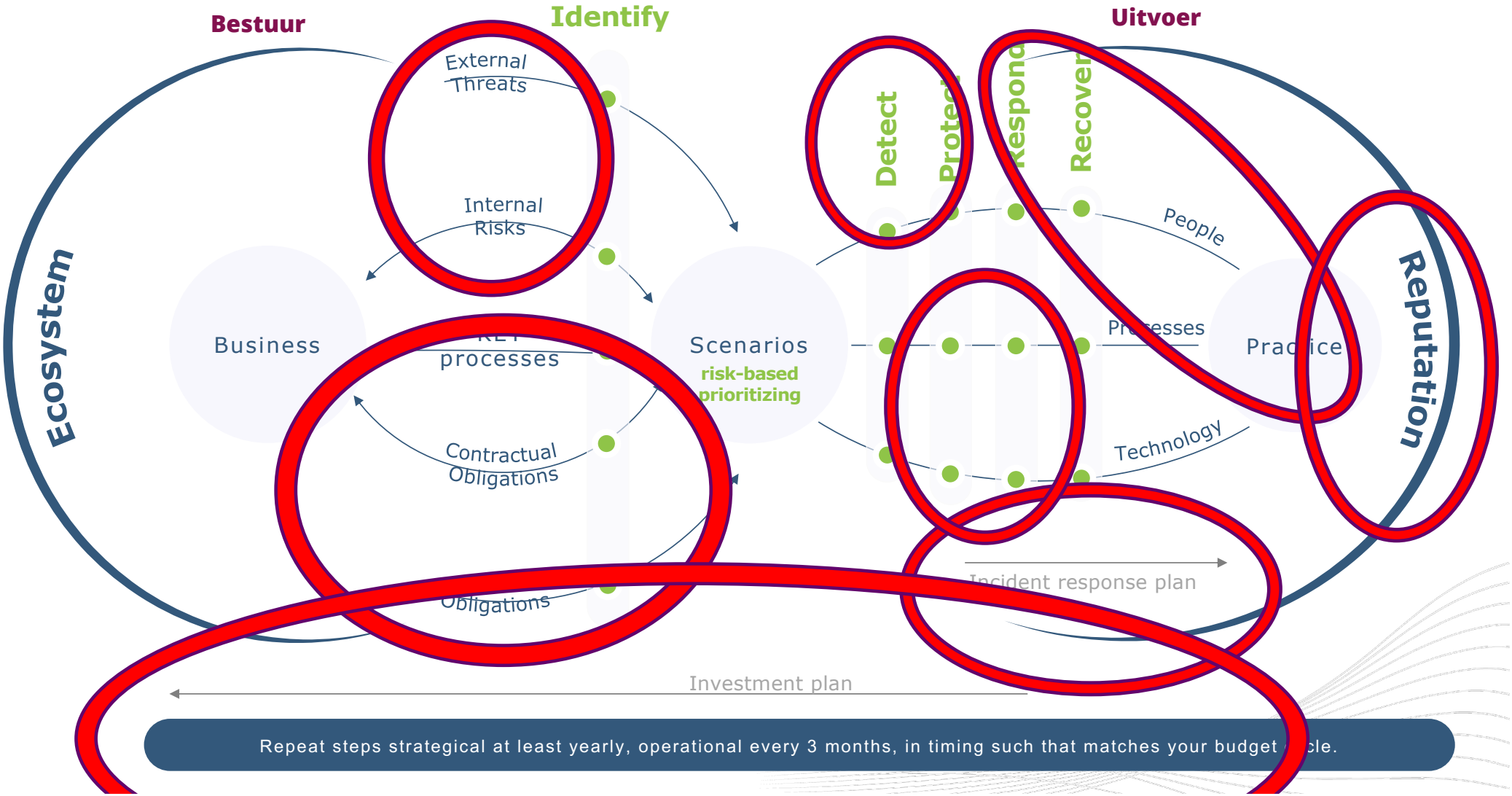
Heb je iemand in je netwerk die je vertrouwt en de trends in de gaten kan houden?
=> Wellicht een IQonIQ leerkring?

Cyber Governance Model



Repeat steps strategical at least yearly, operational every 3 months, in timing such that matches your budget cycle.

Workshop: Persbericht lezen (VDL)



- Werk **risicogebaseerd** aan cyber-volwassenheid, ook voor de NIS-2.

- Leg verantwoordelijkheden op de juiste plek. **Bestuur / uitvoer**

- Bevraag in een vroeg stadium je klanten voor (standaard in) **aantoonbaarheid.**

- Betrek **legal en inkoop,** vooruitlopend op de CRA, het kan je een voorsprong geven.

- Hou het CCV (hetccv.nl) in de gaten voor standaardisatie.

Heb je iemand in je netwerk die je vertrouwt en de trends in de gaten kan houden?

THE CYBER PARTNERS