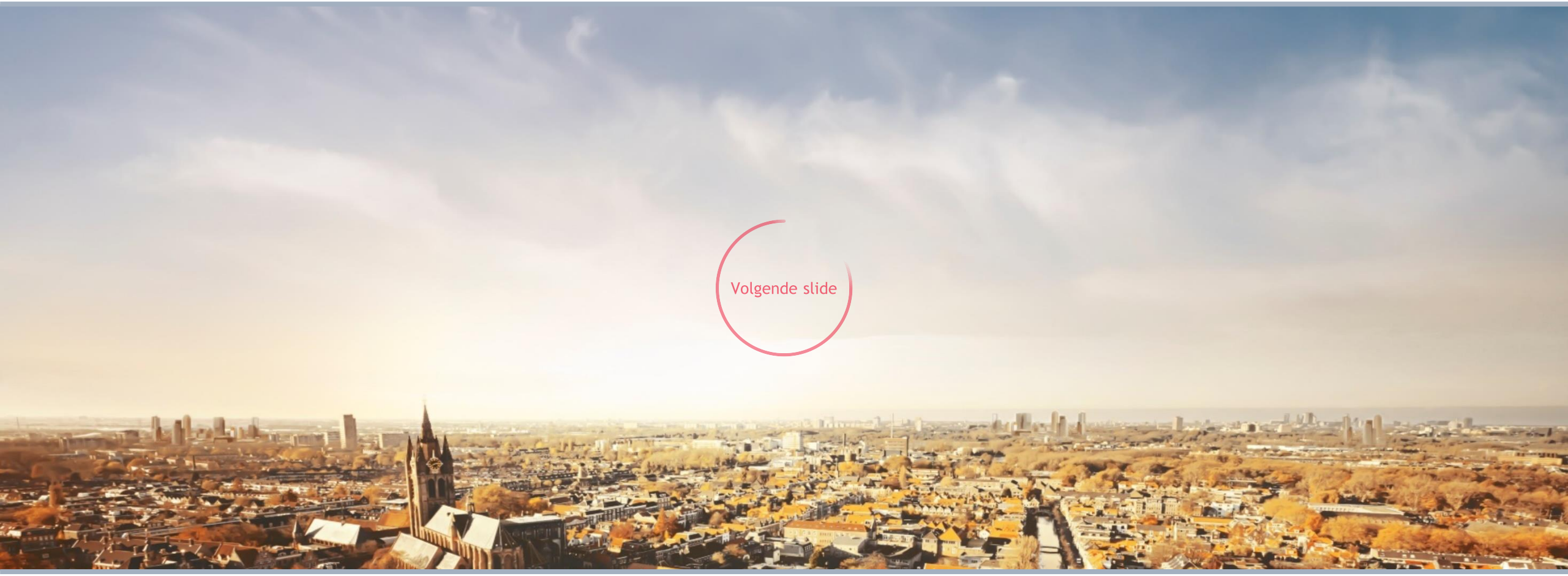
Een digitale aanval, wat nu?

Pensioenfederatie



Oktober 2020

BDO

Introductie

Dirk de Hen

Partner, Forensic Technology

M: +31 (6) 22 420 248

E: dirk.de.hen@bdo.nl

Incident Response Services

Incident Response

Wie is het eerste aanspreekpunt als zich tekenen van een cyber incident voordoen? Bent u voorbereid op een cyberaanval die uw infrastructuur in gevaar brengt?

Van recente incidenten leren we dat organisaties zich niet moeten afvragen óf een beveiligingsincident gaat plaatsvinden, maar wanneer. Dit komt doordat organisaties het altijd aan het juiste eind moeten hebben wat betreft het volledig beschermen van hun bezittingen en processen. Een aanvaller hoeft het namelijk maar één keer goed te hebben om aanzienlijke schade te veroorzaken bij een organisatie.

Organisaties moeten hun aandacht richten op de voorbereiding van kritieke incidenten, aangezien het garanderen van preventie nauwelijks mogelijk is, laat staan haalbaar. De manier waarop een organisatie omgaat met een aanval heeft direct gevolgen op de totale kosten van een incident. In sommige gevallen kunnen soortgelijke incidenten zelfs mogelijkheden bieden om waarde te creëren voor de stakeholders. Dit is alleen in het geval als de organisatie de incidenten snel en adequaat afhandelt. Om dit voor elkaar te krijgen, moeten organisaties een incident response plan opstellen voordat een incident zich voordoet.

Met onze proactieve incident response services bereiden wij organisaties voor op een incident. Door dit te doen, wordt het risico op imago-en financiële schade verminderend, wordt de business continuïteit verbeterd en kunnen de bedrijfsactiviteiten tegelijkertijd voldoen aan de AVG-voorschriften. Mocht het toch misgaan, dan kunt u op ons rekenen om uw organisatie door de kritieke fases na een incident te leiden.

Incident Readiness

Omgeving & stakeholders

- Risico
- Bedrijfscontinuïteit
- Reputatie
- Wet- en regelgeving
- Financieel

Cybersecurity is *niet alleen* de verantwoordelijkheid van IT.

Een incident heeft effect op de gehele organisatie. Het is daarom noodzakelijk dat het incident response team uit vertegenwoordigers bestaat die uit alle afdelingen binnen de organisatie komen.

Aanpak Incident Response

Beoordelen, verbeteren, ondersteunen en feedback

1 Kick off

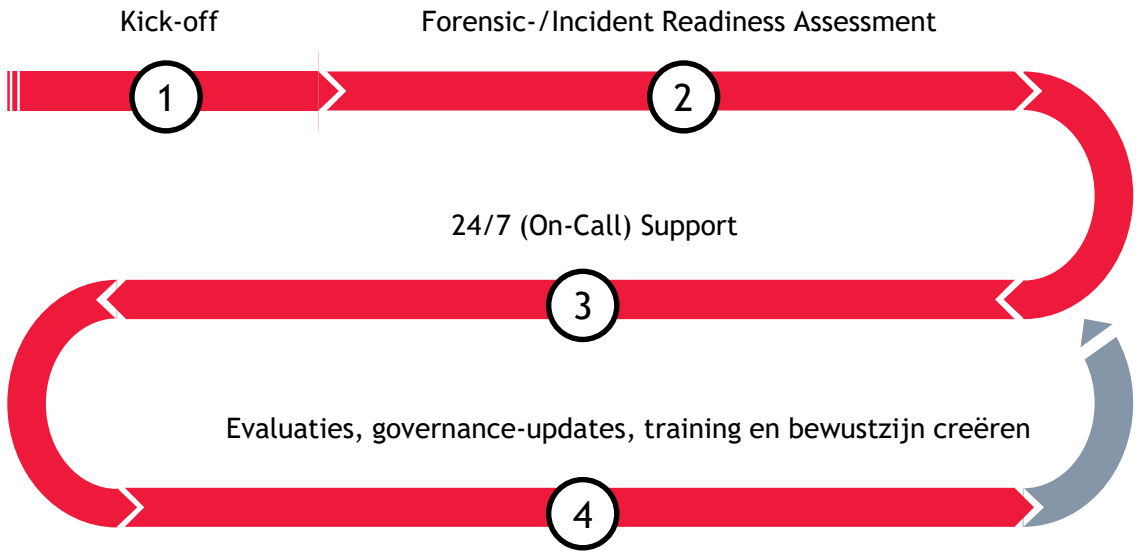
Activiteiten:
- Scope definiëren;
- Incident response maturity assessment.

Deliverable:
- Scope beschrijving;
- Projectplan for IR-implementatie.

3 24/7 On-Call Support

Activiteiten/werkzaamheden:
- Containment activities;
- Remediation activities;
- Onderzoeksondersteuning.

Deliverable:
- Advies en ondersteuning bij het beheren van incidenten;
- Rapportage van bevindingen;
- Ondersteuning bij het melden aan autoriteiten.



2 Forensic-/Incident Readiness assessment

Activiteiten:
- Interviews met key-stakeholders;
- Heatmap van infrastructuur;
- Herzien van huidig beleid en procedures;
- Externe leveranciers;
- Technische beoordeling van de aanwezigheid en inrichting van logging.

Deliverable:
- Incident Response playbook

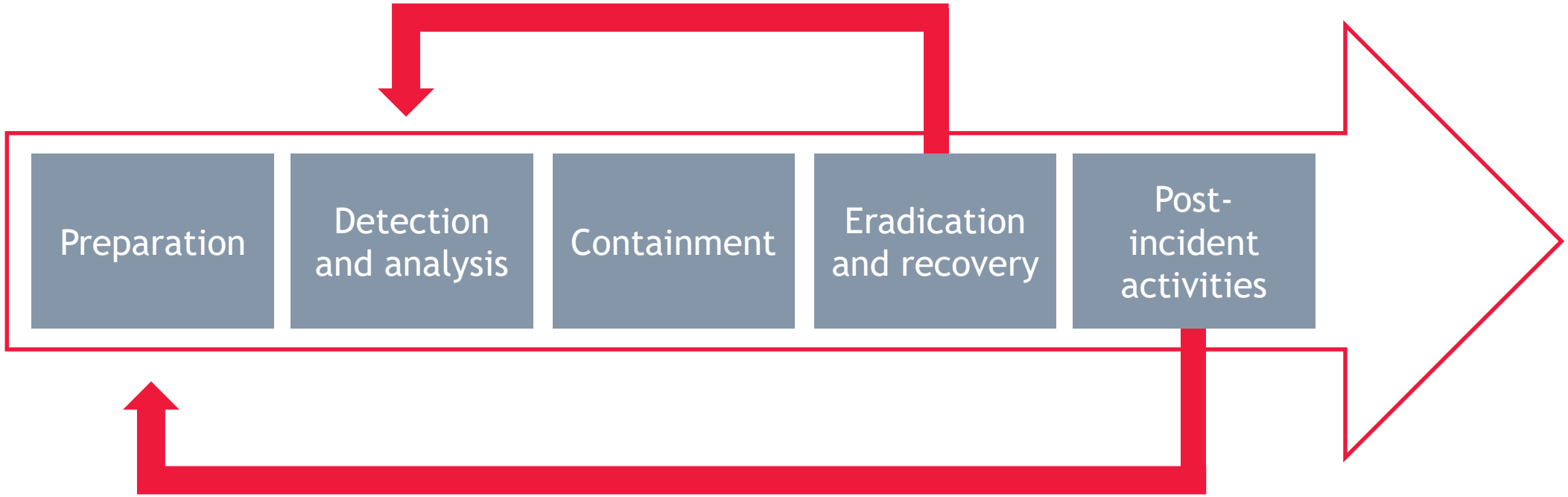
4 Evaluaties, governance-updates, training en bewustzijn creëren

Activiteiten/werkzaamheden:
- Updaten van IR-documentatie;
- First responder-training;
- Bewustwording vergroten door simulaties en ‘fire drills’;
- evaluatie van incidenten en activiteiten.

Deliverables:
- Up-to-date IR-documentatie;
- Fit for purpose IR-organisatie

Incident Response

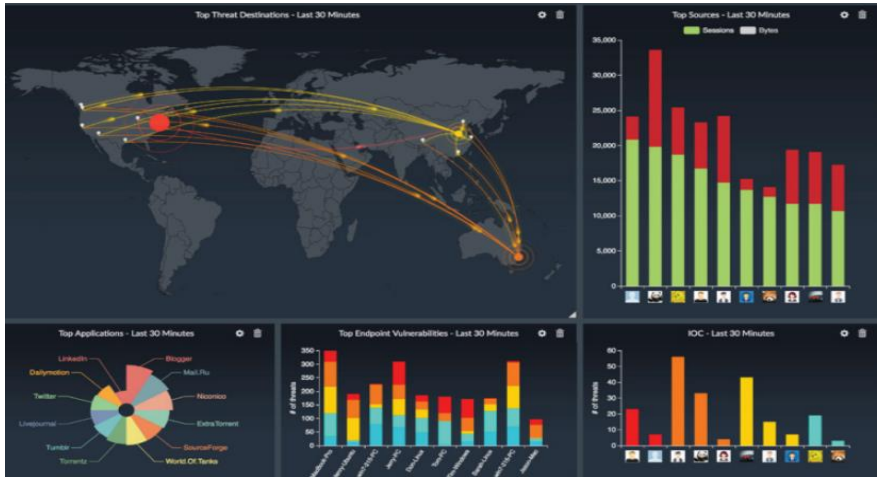
Aanpak

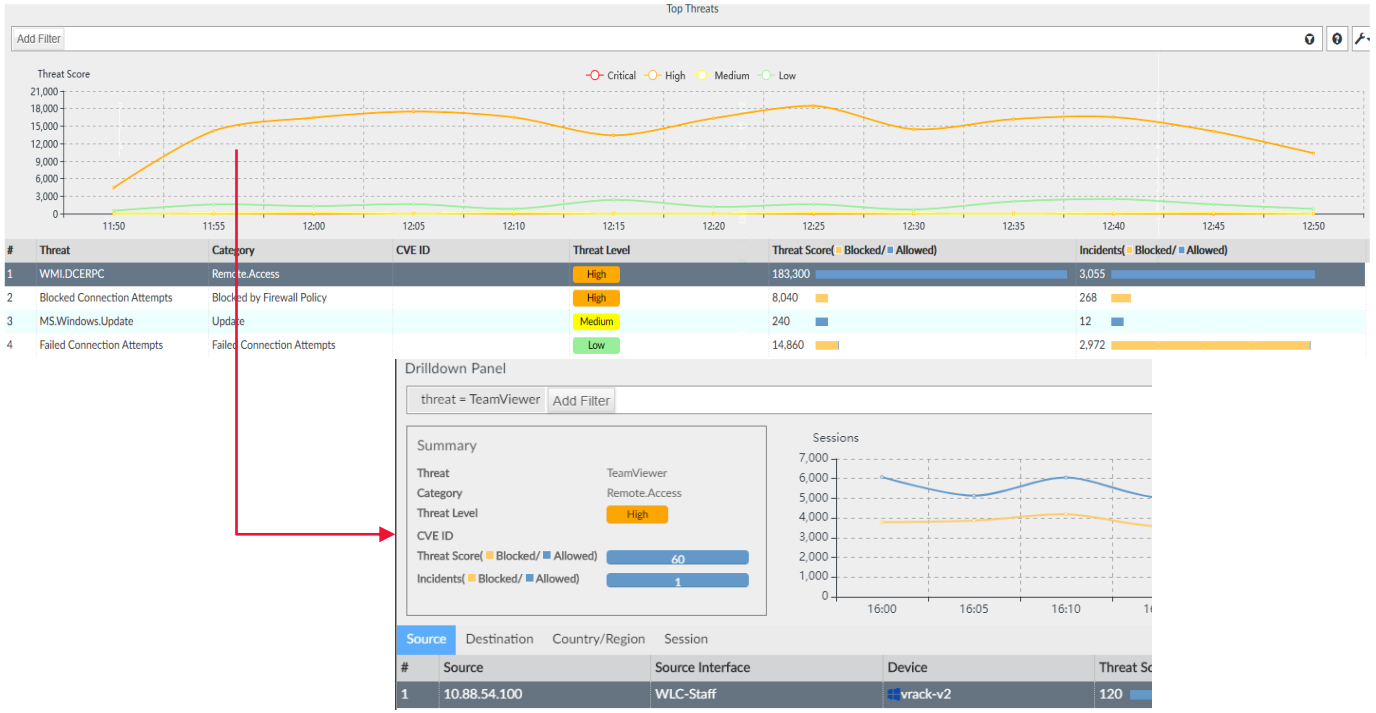


Detectie en analyse

BDO Detection Sensor

- Geen interferentie met netwerkverkeer
- Detection sensor omvat:
  - Detectie van bedreigingen
  - Inzicht in gebruikte applicaties
  - Inzicht in bezochte websites
  - Virus detectie
- Gedetailleerde rapportages





Beheer van datalekken

Tijdlijnen rapportagevereisten

Datalek	Bewust van het lek	Onderzoek naar het lek	Waarschuw toezichthouder (indien er kans is op risico's voor particulieren)	Informeer betrokkenen (indien dit leidt tot risico's voor individuen)
			Zonder onnodige vertraging (niet later dan 72 uur)	Zonder onnodige vertraging

- Dataverwerkers moeten inbreuk op persoonsgegevens aan gegevensbeheerders melden.
- Gegevensbeheerders moeten inbreuk op persoonsgegevens melden aan hun toezichthouders en in sommige gevallen volgens de AVG-bepalingen ook aan bepaalde betrokken personen.
- Gegevensbeheerders registreren het incident in een registratie register.
- Het niet naleven kan leiden tot boetes.

Datalekmanagement

Voorlopige notificatie

Lek wordt gedetecteerd

Onderzoek van het lek

Bewustwording van lek

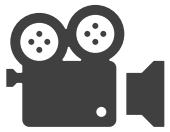
Bewustwording van kwaadwillende handelingen:

Interne

werknemer

klokkenluider

Externally



Media

Externe partij

Autoriteiten

Beoordeel de risico's die door het lek ontstaan; welke factoren kunnen als risico worden beschouwd:

- Type lek, toegang tot meer bronnen van PI?
- De aard en gevoeligheid van en de hoeveelheid informatie.
- Is de identificatie van de getroffen personen gemakkelijk te vinden?
- Ernst van de gevolgen voor individuen.
- Aantal getroffen individuen.

Elk lek en alle relevante en beschikbare informatie wordt vastgelegd in de Data Privacy Tool of het Data Breach Register. Dit zorgt ervoor dat:

- de privacy is gewaarborgd;
- alle relevante belanghebbenden op de hoogte worden gesteld.

Tips naar aanleiding van casus

- Monitor actief het netwerk verkeer
- Monitor de aanmaak van automatische ‘rules’ op mailboxen
- Verifieer dat de logging door systemen juist is ingeregeld
- Verifieer een bankrekeningnummer wijziging altijd via een ander medium
- Implementeer een incident response plan
- Toets jaarlijks de werking van het incident response plan
- Evalueer incidenten om verbeterpunten te identificeren
- Organiseer kennis om adequaat te kunnen reageren op een incident
- Implementeer een praktische en pragmatische oplossing voor incident response

Are you prepared?

How prepared are you?

Vragen?

Bedankt voor uw aandacht