# Data Assessment In-A-Day

## Bepaal het optimale bereik van uw Privacy Impact Assessment


## Samenvatting

**Vanaf 1 Juli 2015 is Meldplicht Datalekken van kracht gegaan ter voorbereiding op de nieuwe Europese Privacy Verordening en wordt verwacht dat u als bedrijf daaraan gaat voldoen. Om te bepalen wat de impact is van deze nieuwe verordening op uw bedrijf kunt u een Privacy Impact Assessment (PIA) uitvoeren of laten uitvoeren. Een PIA is een methode om privacy risico's op gestructureerde wijze in kaart te brengen rondom ICT-systemen en databestanden. Van groot belang hierbij is de wijze waarop de systemen informatie uitwisselen: de datastromen. Veel bedrijven hebben echter niet in beeld hoe deze datastromen lopen. Met behulp van ons Data Assessment in-a-day maakt Cyber4Z de datastromen in uw omgeving inzichtelijk. Hiermee kunt u bepalen wat de scope van uw PIA wordt, zodat die sneller en efficiënter kan worden uitgevoerd.**


## Data in rest en data in transit

In veel van de situaties die wij tegen komen is het bedrijf dat een PIA uitvoert niet op de hoogte van datastromen die interactie hebben buiten het bedrijf, laat staan dat men weet welke inhoud het bedrijf verlaat. Voordat het bereik van een PIA kan worden vastgesteld is het van belang om inzicht te hebben in deze datastromen.

Applicaties, systemen en netwerkelementen gebruiken data. Veel van deze data is ergens opgeslagen en wordt pas gebruikt indien dat voor de functie noodzakelijk is. Dit noemen we de **data in rest.** Vaak weet een organisatie niet welke data waar staat totdat deze effectief wordt gebruikt.

Als data vervolgens wordt bewerkt, zal het van een object naar een subject worden verplaatst. Dit kan handmatig of automatisch en noemen we **data in transit**. Veel van die data wordt tegenwoordig al vercijferd zodat deze niet leesbaar is, maar dat geldt niet voor alle data. Als de data dan vercijferd is, is het vaak ook niet duidelijk wie er in het bezit is van het sleutelmateriaal. (Zie daarvoor ook Key-Assessment In-a-Day)

## De verwerking van Data

Data die uiteindelijk wordt verwerkt in een applicatie, operating systeem, database of netwerkelement zal leesbaar zijn, omdat er op dit moment geen methode beschikbaar is waarmee vercijferde data direct kan worden verwerkt. Dit is vaak het moment dat privacy gevoelige data ook leesbaar is door de verwerker. Het moment van verwerken van data wordt vaak door hackers gebruikt om de voor hun waardevolle informatie over een onderwerp of persoon te kunnen verkrijgen.

## Wat levert het u op?

Cyber4Z maakt gebruik van een van haar partners om, door middel van tooling, de datastromen inzichtelijk te maken in een architectuur. Het gaat dan om die datastromen die van binnen de organisatie wordt verplaatst (data in transit) naar buiten. Op basis van deze resultaten vindt vervolgens het uiteindelijke assessment plaats waarbij de datastromen door specialisten van Cyber4Z worden geanalyseerd.

Het resultaat van deze analyse is een uitgebreid overzicht van interne naar externe datastromen. Voor de uitvoering van de Privacy Impact Assessment is het dan duidelijk waar de data naar toe gaat en wie de data uiteindelijk in zou kunnen zien. Op basis van deze informatie kan ook worden vastgesteld wat het doel is van deze datastromen. Deze analyse is van aanzienlijk belang voor de Privacy Impact Assessment omdat hiermee de scope van de PIA kan worden bepaald.

Het inzichtelijk maken zou ook kunnen aan de hand van een inventarisatie van de IP gerelateerde bedrijfsmiddelen met behulp van een analyse op basis van inzet van zogenaamde 'sniffers'. Op deze manier is echter nooit zeker of de analyse compleet is. Daarnaast is deze wijze van analyse relatief duur.

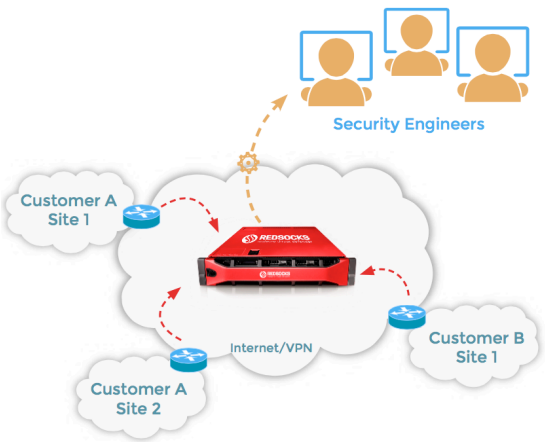
## Voordelen van het assessment

- U krijgt inzicht in de datastromen die nodig zijn voor een adequate uitvoering van de PIA;
- U maakt aantoonbaar welke datastromen uw bedrijf verlaten en welke datastromen met bevoegde interne instanties interactie hebben;
- U maakt aantoonbaar welke datastromen extra

- aandacht nodig hebben voor uw Privacy Impact Assessment;
- U bespaart veel tijd en geld, omdat de datastromen niet handmatig geanalyseerd hoeven te worden;
- Naast de gegevens over de datastromen is het tevens mogelijk om aan te tonen of hackers al zijn binnengedrongen in uw domein.

## De uitvoering

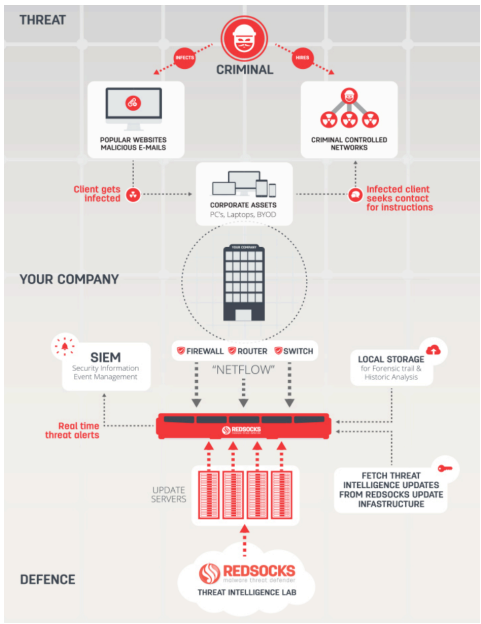
Voor de uitvoering wordt de Redsocks Malware Threat Defender toegepast die een dag meedraait in uw netwerk. De locatie van de MTD is parallel aan de router die het netwerk verdeeld en binnen de scope van het assessment valt. Dit is in de tekening weergegeven. De router levert metadata aan de MTD over het netwerkverkeer. Metadata betreft niet de inhoud van de communicatie zelf, maar de aard ervan zoals adres van de afzender en ontvanger, het protocol, de gebruikte poort(en) en de omvang ervan.




Na die dag zal door een specialist van Cyber4Z een analyse worden uitgevoerd en een rapport worden opgemaakt. Dit rapport wordt gepresenteerd aan het MT van de organisatie

## Compliance

De inhoud van de data wordt door de MTD niet bekeken. Er wordt alleen inzicht gegeven in de datastromen met behoud van privacy. De gebruikte tooling is compliant met de wet- en regelgeving omtrent datalekken.




Deze assessment is mogelijk gemaakt door :

REDSOCKS
malware threat defender

Voor meer informatie kunt u contact opnemen met ons via 4z4u@cyber4z.com of u belt Rob Mellegers, Algemeen Directeur Cyber4Z, rob.mellegers@cyber4z.com, +31-(0)643587481

**CYBER4Z**
Ernani 21
5629 NB Eindhoven

**www.cyber4z.com**

Cyber4Z Helps our clients to reach their strategic goals by mitigating IT Risks in order to profit the use of IT maximally.