///Geo-blocking

1 INTRODUCTIE

Cybercriminelen komen voor in elke geografische regio ter wereld. Er zijn regio's die bijvoorbeeld door hun geopolitieke situatie of nalatig internettoezicht een groter risico vormen voor de cyberveiligheid van uw medewerkers en IT-systemen, juist om dit risico te verkleinen kunt u geo-blocking toepassen.

Geo-blocking is een technologie die de internettoegang kan beperken op basis van gebruikers hun geografische locatie. Dit kan zowel voor inkomend als uitgaand verkeer. Door IP-adressen van bepaalde geografische regio's toe te voegen aan de uitgaande firewall regels van uw organisatie, kunnen uw medewerkers geen webservices met deze specifieke IP-adressen bezoeken.

Door diezelfde IP-adressen toe te voegen aan de inkomende firewall regels, kunnen internetgebruikers met deze specifieke IP-adressen uw websites niet meer bereiken. Geo-blocking wordt vooral gebruikt om kopierecht en licentie fraude op het internet te voorkomen (bijv. door streamingsdiensten), maar wordt ook toegepast door organisaties om het risico op misbruik te verkleinen.

2 WET- EN REGELGEVING

Geo-blocking is toegestaan voor Belgische lokale besturen mits er voldaan wordt aan de Europese Geo-blocking Regulation[1]. De in 2018 geadopteerde regelgeving schrijft voor dat het verboden is om ongeoorloofd geo-blockingt oe te passen in de Europese Unie. Ongeoorloofde geo-blocking verwijst naar situaties waarin bedrijven binnen de Europese Unie doelbewust de prijzen van hun producten of diensten verhogen voor buitenlandse (online) klanten of websites en applicaties ontoegankelijk maken voor buitenlandse gebruikers.

In principe heeft de Geo-blocking Verordening niet veel invloed op het doorvoeren van geo-blocking bij lokale besturen, maar het is wel iets om in de gaten te houden wanneer u als lokaal bestuur de IP-adressen van een regio die binnen de Europese Unie ligt, wilt blokkeren. Om ervoor te zorgen dat de algemene toepassingen van uw lokaal bestuur (bijv. uw website) vanuit heel de Europese Unie toegankelijk zijn, wordt het aanbevolen om geo-blocking enkel toe te passen voor toegang tot kritische applicaties of geprivilegieerde toegangen.

[1] Regulation (EU) 2018/302

3 AANBEVELINGEN

Het Vo-CRT raadt lokale besturen aan om geo-blocking toe te passen (zowel voor inkomend en uitgaand internetverkeer) op alle informatiestromen die instaan voor het beheer van uw infrastructuur op afstand.

Inkomend internetverkeer geo-blocken

Vanuit de Vlaamse overheid bestaat er geen lijst met IP-adressen of geografische regio's die geblokkeerd zouden moeten worden. In plaats daarvan bieden de meeste (webapplicatie) firewall leveranciers (al dan niet betalende) opties aan om geo-blocking toe te passen. Vaak bevatten deze opties ook detectie op 'impossible travel'. Impossible travel detectie vergelijkt de meest recent gebruikte IP-adressen of GPS-adressen van één gebruiker. Indien het reisgedrag van een gebruiker afwijkt of fysiek niet mogelijk is (bijv. door in 20 minuten in te loggen vanuit Brussel en Los Angeles), kan er een waarschuwing verstuurd worden naar de gebruiker of wordt het account tijdelijk opgeschort. Hierdoor kan de legitieme eigenaar van het account actie ondernemen of wordt de cybercrimineel buitenspel gezet.

Er wordt geadviseerd om geo-blocking en impossible travel detectie ten minste te activeren voor alle communicaties die instaan voor het beheer van de infrastructuur op afstand. Het is belangrijk om geo-blocking altijd te combineren met reguliere controles op ongewenste IP-adressen. Geo-blocking kan ook toegepast worden op reguliere gebruikers toepassingen maar gezien het brede publiek dat de websites van uw lokaal bestuur bezoekt, is dit niet altijd mogelijk.

Uitgaand internetverkeer geo-blocken

Om ervoor te zorgen dat uw medewerkers geen frauduleuze websites bezoeken via uw netwerken, wordt er geadviseerd om geo-blocking ook op uitgaand internetverkeer toe te passen. Uitgaand internetverkeer kan gereguleerd worden door middel van DNS Sinkholes. Een DNS Sinkhole is een DNS server op netwerkniveau die geconfigureerd is om DNS aanvragen van een vooraf bepaalde lijst van domeinen te blackholen. Dit betekent dat de DNS server deze specifieke DNS aanvragen onderschept en de aanvrager een fout IP-adres teruggeeft. In de praktijk resulteert dit in een foutmelding bij de gebruiker wanneer hij of zij naar de geblokkeerde domeinen surft.

Ook voor uitgaand internetverkeer bieden de meeste dienstenleveranciers services aan om DNS Sinkholing toe te passen of kunnen zij uw IT-team voorzien van regulier geüpdatete domein lijsten. Zo kan uw IT-team deze domein lijst gebruiken om de DNS server op een juiste manier te configureren.

Geoblocking omzeilen

Vanuit de Vlaamse overheid wordt geadviseerd om geo-blocking toe te passen. Kwaadwilligen kunnen geo-blocking omzeilen door gebruik te maken van Virtual Private Networks (VPN). VPN zorgt voor een beveiligde, versleutelde en anonieme verbinding tussen de gebruiker en het internet. Ook kan de gebruiker een internetverbinding opzetten vanuit een ander land dan het land waar hij/zij zich daadwerkelijk bevindt. Zo is het

bijvoorbeeld mogelijk om vanuit Nederland een internetverbinding op te zetten die de indruk geeft uit België te komen. Omdat geo-blocking kan omzeild worden, moet u de methode niet gebruiken als primaire beveiliging van uw netwerken en infrastructuur, maar meer als een middel om de diepte van uw beveiliging te vergroten.

4 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
Geo-blocking	Geo-blocking verwijst naar het blokkeren of beperken van de toegang tot websites, apps en andere internetcontent in functie van de geografische locatie van de gebruikers	Geo-blocking in de Europese Unie | FOD Economie (fgov.be)
DNS	De term DNS verwijst naar Domain Name System. DNS is een netwerkprotocol dat op het internet gebruikt wordt om namen van computers naar IP-adressen te vertalen en omgekeerd.	DNS Sinkhole — ENISA (europa.eu)
DNS Sinkhole	De term DNS Sinkhole verwijst naar Domain Name System Sinkhole. Een DNS Sinkhole is een Domain Name Server die geconfigureerd is om valse DNS resultaten te geven voor vooraf bepaalde DNS.	DNS Sinkhole — ENISA (europa.eu)

5 REFERENTIES

- Europese Geo-blocking Verordening

https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32018R0302&from=EN