

/// Aanbevelingen voor het blokkeren van TikTok van uw lokaal bestuur

1 CONTEXT

In navolging van het besluit om de toegang tot de applicatie TikTok te blokkeren voor alle overheden die gebruik maken van de gemeenschappelijke IT-dienstverlening en het netwerk van de Vlaamse overheid, heeft het Crisismanagementteam (CMT) van het Crisiscentrum van de Vlaamse overheid (CCVO) besloten tot een verbod op de installatie en het gebruik van de applicatie TikTok op alle vaste en mobiele diensttoestellen van personeelsleden van de Vlaamse overheid.

Op basis van het besluit van het Crisismanagementteam (CMT), raadt het Vo-CRT aan om ook binnen uw lokaal bestuur de applicatie TikTok te blokkeren op uw netwerk en op de diensttoestellen van uw personeelsleden. In dit artikel wordt er kort stil gestaan bij de wet- en regelgeving en worden er twee technieken uitgelegd waarmee uw lokaal bestuur TikTok van het netwerk kan blokkeren.

2 WET- EN REGELGEVING

Hoewel er geen wettelijk of regelgevend kader is voor het verbod op TikTok, heeft de Vlaamse overheid zich gebaseerd op de adviezen van het Centrum voor Cybersecurity Belgium (CCB), de Algemene Dienst Inlichting en Veiligheid (ADIV) en de Veiligheid van de Staat (VVSE). De bezorgdheid van deze diensten rond TikTok, hebben betrekking op de vergaring van data, het delen van deze data met de Chinese overheid en beïnvloeding. Het vermoeden leeft dat TikTok data verzamelt (informatie uit open bronnen), wat zou kunnen leiden tot het buit maken van creditcard nummers en wachtwoorden. Deze dataverzameling zou volgens enkele onderzoekers gebeuren in grote hoeveelheden en zonder expliciete toestemming van gebruikers wat in tegenspraak is met de Algemene Verordening Gegevensbescherming (AVG). Daarbij komt nog dat er een grote bezorgdheid leeft rond de privacy van minderjarigen, een grote doelgroep voor TikTok.

Meer informatie hierover:

<https://ccb.belgium.be/sites/default/files/TikTok%20Advies%20NL%20V3b.pdf>

3 AANBEVELINGEN

Het Vo-CRT raadt lokale besturen aan om het advies van de Vlaamse overheid te volgen en TikTok op hun netwerken te verbieden. Het Vo-CRT heeft twee bewezen technieken geïdentificeerd: het opzetten van een DNS Sinkhole en het modifieren van de firewall. Beide technieken worden hieronder meer in detail uiteengezet. De twee technieken kunnen tegelijkertijd worden gebruikt en zo nog meer veiligheid garanderen.

DNS Sinkhole

Lokale besturen kunnen beslissen om een DNS Sinkhole of DNS blackhole op te zetten. 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 domeinen van bv. TikTok probeert te gaan.

Een DNS Sinkhole kan ook worden opgezet op toestel niveau. Het toestel controleert dan voordat het een aanvraag doet aan de DNS server of het domein connecteerd is naar een Sinkhole IP. U kan specifieke domeinen connecteren naar een Sinkhole IP door uw local hosts file te veranderen en daarin de gewenste domeinen te benoemen.

Vanuit de Vlaamse overheid zouden de volgende domeinen geblokkeerd moeten worden:

- *.tiktok.com
- *.tiktokcdn.com
- *.tiktokv.com
- *.musical.ly
- p16-tiktokcdn-com.akamaized.net

Firewall

Op firewall niveau kunt u het gebruik van TikTok blokkeren door klassieke IP-filters op de firewall te plaatsen. Door het plaatsen van IP-filters wordt een ongewenste data uitwisseling tussen uw netwerk en de specifieke IP-adressen geblokkeerd. Hierdoor kunnen gebruikers van uw netwerk TikTok niet meer gebruiken.

Vanuit de Vlaamse overheid zouden de volgende IP-adressen moeten geblokkeerd worden:

- 161.117.70.145
- 161.117.71.36
- 161.117.71.33
- 161.117.70.136
- 161.117.71.74
- 216.58.207.0/24
- 47.89.136.0/24
- 47.252.50.0/24
- 205.251.194.210
- 205.251.193.184
- 205.251.198.38



- 205.251.197.195
- 185.127.16.0/24
- 182.176.156.0/24

4 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
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.	What is DNS? How DNS works Cloudflare
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.	What is a DNS Sinkhole Malware Detection Netacea

5 REFERENTIES

- Centrum voor Cybersecurity Belgium (CCB) berichtgeving rond het blokkeren van TikTok: <https://ccb.belgium.be/sites/default/files/TikTok%20Advies%20NL%20V3b.pdf>
- Digitaal Vlaanderen – Privacy en gegevensbescherming [“Privacy en gegevensbescherming is iets wat iedereen aanbelangt” | Vlaanderen.be](#)

