Ministerie van Veiligheid en Justitie

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
708641

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Datum 4 januari 2016
Onderwerp Kabinetsstandpunt encryptie

Kabinetsstandpunt Encryptie
Hierbij sturen wij u het kabinetsstandpunt toe over encryptie. Hiermee wordt tegemoet gekomen aan de gedane toezeggingen tijdens het AO Telecomraad van 10 juni 2015 (TK 2014-2015, 21501-33, nr. 552) en AO JBZ-Raad van 7 oktober 2015.

Inleiding
Encryptie, ook wel versleuteling, is in toenemende mate eenvoudig te verkrijgen en gebruiken en maakt daarmee steeds vaker onderdeel uit van het reguliere dataverkeer. Door de overheid, bedrijven en burgers wordt encryptie steeds meer toegepast om de vertrouwelijkheid en integriteit van hun communicatie en opgeslagen data te beschermen. Dat is belangrijk voor het vertrouwen van mensen in digitale producten en diensten en voor de Nederlandse economie in het licht van de zich snel ontwikkelende digitale maatschappij. Tegelijkertijd vormt encryptie een belemmering voor het verkrijgen van informatie die noodzakelijk is voor opsporings-, inlichtingen- en veiligheidsdiensten wanneer kwaadwillenden (zoals criminelen en terroristen) hiervan gebruikmaken. De recente aanslagen in Parijs, waarbij mogelijk gebruik is gemaakt van versleuteling van de communicatie door de terroristen, leiden tot de gerechtvaardigde vraag wat er nodig is om opsporings-, inlichtingen- en veiligheidsdiensten goed zicht te bieden en laten houden op aanslagplanning.

De in de vorige alinea beschreven tweeledigheid was eveneens te horen in het publieke debat van de afgelopen maanden over de dilemma's rondom het gebruik van encryptie. Ook uw Kamer heeft over dit onderwerp gesproken. Tijdens het AO Telecomraad is gevraagd wat het Kabinet gaat doen aan het stimuleren van sterke encryptie. Daarnaast is vanuit de Tweede Kamer gevraagd om te komen met een kabinetsstandpunt rond encryptie.

Hierna wordt ingegaan op het belang van encryptie voor de systeem- en informatiebeveiliging van de overheid en bedrijven, en voor de grondwettelijke bescherming van de persoonlijke levenssfeer en het communicatiegeheim. Daarnaast wordt het belang van opsporing van ernstige misdrijven en bescherming van de nationale veiligheid geschetst. Tot slot wordt na weging van de belangen gekomen tot een conclusie.

De Nederlandse situatie kan hierbij niet los worden gezien van de internationale context. Sterke encryptiesoftware is in toenemende mate wereldwijd beschikbaar of al geïntegreerd in producten of diensten. Gelet op de brede beschikbaarheid en toepassing van geavanceerde encryptietechnieken en het grensoverschrijdende karakter van het dataverkeer is het handelingsperspectief op nationaal niveau beperkt.

Belang van encryptie voor de overheid, bedrijven en burgers
Cryptografie speelt een sleutelrol in de technische beveiliging in het digitale domein. Veel cybersecuritymaatregelen in organisaties leunen sterk op de toepassing van encryptie. De veilige opslag van wachtwoorden, het beschermen van laptops tegen verlies of diefstal en het veilig bewaren van backups zijn moeilijker zonder het gebruik van encryptie. Het afschermen van gegevens die verstuurd worden via internet, bij internetbankieren bijvoorbeeld, is alleen mogelijk met behulp van encryptie. Door de verbondenheid van systemen, wereldwijde vertakkingen en verschillende routes die communicatie kan afleggen, is het risico op onderschepping, inbreuk, inzage of wijziging van informatie en communicatie altijd aanwezig.

De overheid communiceert in toenemende mate digitaal met de burgers en verleent diensten waarbij vertrouwelijke gegevens worden uitgewisseld, zoals het gebruik van DigiD of het doen van belastingaangifte. Zoals in het Regeerakkoord is geformuleerd moeten vanaf 2017 burgers en bedrijven hun overheidszaken volledig digitaal kunnen regelen. De overheid heeft hierbij de plicht om te zorgen dat deze gegevens tegen kennisneming door derden zijn beveiligd; encryptie is hiervoor onontbeerlijk. Ook de bescherming van de communicatie binnen de overheid is van encryptie afhankelijk zoals bij de beveiliging van diplomatiek berichtenverkeer en militaire communicatie.

Voor bedrijven is encryptie essentieel om bedrijfsinformatie veilig te kunnen bewaren en versturen. Het kunnen gebruiken van encryptie versterkt de internationale concurrentiepositie van Nederland en draagt bij aan een aantrekkelijk vestigings- en innovatieklimaat voor onder andere startups, datacentra en cloudcomputing. Vertrouwen in veilige communicatie en opslag van data is essentieel voor de (toekomstige) groeipotentie van de Nederlandse economie, die vooral zit in de digitale economie.

Encryptie ondersteunt de eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers doordat het hen een middel biedt om de vertrouwelijkheid en integriteit van persoonsgegevens en communicatie te beschermen. Dit is ook belangrijk voor de uitoefening van de vrijheid van meningsuiting. Het stelt bijvoorbeeld burgers, maar ook beroepen met een belangrijke democratische functie zoals journalisten, in staat om vertrouwelijk te communiceren.

Encryptie stelt derhalve alle betrokkenen in staat de vertrouwelijkheid en integriteit van communicatie te waarborgen en zich beter te weren tegen bijvoorbeeld spionage en cybercriminaliteit. Hierbij zijn fundamentele rechten en vrijheden, veiligheids- en economische belangen gebaat.

Encryptie en de opsporings–, inlichtingen- en veiligheidsdiensten

De bevoegdheden en middelen die de diensten tot hun beschikking hebben, moeten toegerust zijn op de huidige en toekomstige digitale realiteit. Met effectieve, rechtmatige toegang tot gegevens bevorderen de opsporings-, inlichtingen- en veiligheidsdiensten de veiligheid van de digitale en de fysieke wereld. Encryptie vormt waar het toegepast wordt door kwaadwillenden een belemmering voor de opsporings-, inlichtingen- en veiligheidsdiensten bij de toegang tot die gegevens. Zij ervaren deze belemmeringen bijvoorbeeld wanneer zij onderzoek doen naar de verspreiding en opslag van kinderporno, bij de ondersteuning van militaire missies in het buitenland, het tegengaan van cyberaanvallen of wanneer zij zicht willen krijgen en houden op het voorbereiden van aanslagen door terroristen. Criminelen, terroristen en tegenstanders in gewapende conflicten zijn zich er vaak van bewust dat zij op enig moment de aandacht van de diensten kunnen trekken en hebben tegenwoordig eveneens beschikking over geavanceerde encryptiemethoden die lastig te omzeilen of doorbreken zijn. Het gebruik van dergelijke methoden vereist weinig technische kennis, aangezien encryptie vaak integraal deel uitmaakt van de internetdiensten waarvan ook zij gebruik kunnen maken. Dat bemoeilijkt, vertraagt, of maakt het onmogelijk om (tijdig) inzicht te verkrijgen in de communicatie ten behoeve van de bescherming van de nationale veiligheid en de opsporing van strafbare feiten. Tevens kan het onderzoek ter zitting en de bewijsvoering voor een veroordeling ernstig worden gehinderd.

Het recht op eerbiediging van de persoonlijke levenssfeer en het communicatiegeheim van burgers

Het toepassen van encryptie helpt burgers zoals eerder werd opgemerkt, bij het borgen van de persoonlijke levenssfeer en de vertrouwelijkheid van hun communicatie. De hierboven genoemde rechtmatige toegang tot gegevens en communicatie door opsporings-, inlichtingen- en veiligheidsdiensten vormt evenwel een inbreuk op de vertrouwelijke communicatie van burgers.

Vertrouwelijkheid van communicatie raakt aan de grondwettelijk geregelde eerbiediging van de persoonlijke levenssfeer en aan het recht op bescherming van het brief-, telefoon- en telegraafgeheim (hierna: 'het communicatiegeheim'). Deze grondrechten zijn verankerd in respectievelijk artikel 10 en artikel 13 Grondwet. Daarnaast zijn deze fundamentele rechten vastgelegd in artikel 8 EVRM en artikel 7 en artikel 8 EU-Handvest (voor zover Unierecht wordt geraakt).

De bescherming van grondrechten is van toepassing op de digitale wereld. De hiervoor genoemde grondrechtelijke- en internationaalrechtelijke bepalingen bieden samen het kader om onwettige inbreuken tegen te gaan. De genoemde rechten zijn niet absoluut, hetgeen inhoudt dat beperkingen zijn toegestaan voor zover deze voldoen aan de vereisten die de Grondwet en het EVRM (en voor zover het Unierecht betreft, het EU-Handvest) stellen. Een inbreuk is toelaatbaar wanneer deze een legitiem doel dient, bij wet is geregeld en de beperking voorzienbaar en kenbaar is. Daarnaast dient de beperking noodzakelijk te zijn in een democratische samenleving. Tot slot dient de inbreuk proportioneel te zijn, dat wil zeggen dat het door de overheid nagestreefde doel proportioneel dient te zijn in relatie tot de inbreuk op de persoonlijke levenssfeer en/of het communicatiegeheim.

Deze vereisten bieden het kader waarbinnen de afweging gemaakt kan worden tussen de bij encryptie in het geding zijnde belangen, zoals het recht op de persoonlijke levenssfeer en het communicatiegeheim, de openbare en nationale

veiligheid en het voorkomen van strafbare feiten. Voorgaand afwegingskader is voor zover het de bijzondere bevoegdheden van de inlichtingen- en veiligheidsdiensten betreft overigens ook neergelegd in de Wet op de inlichtingen- en veiligheidsdiensten 2002 (artikelen 18 en 31 van de Wiv 2002). De medewerkingsverplichtingen inzake decryptie die zijn opgenomen in de Wiv (artikelen 24, derde lid en 25, zevende lid van de Wiv 2002) en in het WvSv (artikel 126m, zesde lid, van het WvSv), kunnen worden ingeroepen indien de daaraan gekoppelde bijzondere bevoegdheden na een afweging in voormelde zin worden uitgeoefend.

Afweging en conclusie
Het breken van de versleuteling is tegenwoordig in steeds minder gevallen mogelijk. Daarnaast is de mogelijkheid om gegevens in onversleutelde vorm te vorderen bij een dienstverlener, minder vaak beschikbaar. In toenemende mate worden bij moderne toepassingen van encryptie de gegevens nog slechts in versleutelde vorm door dienstverleners verwerkt. Gelet op het belang van de opsporing en vervolging van strafbare feiten en de belangen die zijn gemoeid met de nationale veiligheid, nopen deze ontwikkelingen tot het zoeken naar nieuwe oplossingen.

Op dit moment is er geen zicht op mogelijkheden om in algemene zin, bijvoorbeeld via standaarden, encryptie producten te verzwakken zonder daarmee de veiligheid van digitale systemen die van encryptie gebruik maken te compromitteren. Door bijvoorbeeld een technische ingang in een encryptie product te introduceren die het voor opsporingsinstanties mogelijk zou maken versleutelde bestanden in te zien, kunnen digitale systemen kwetsbaar worden voor bijvoorbeeld criminelen, terroristen en buitenlandse inlichtingendiensten. Dit zou onwenselijke gevolgen hebben voor de beveiliging van gecommuniceerde en opgeslagen informatie, en de integriteit van ICT-systemen, die in toenemende mate van belang zijn voor het functioneren van de samenleving.

Bij de uitvoering van hun wettelijke taken zijn de opsporings-, inlichtingen- en veiligheidsdiensten deels afhankelijk van samenwerking met aanbieders van ICT-producten en -diensten. Gegeven deze afhankelijkheid, is overleg nodig met aanbieders over effectieve gegevensverstrekking bij gebruik van hun diensten door kwaadwillenden, met inachtneming van ieders rol en verantwoordelijkheden en de wettelijke kaders.

Gegeven de voorgaande afweging komen we tot de volgende conclusie:

Het kabinet heeft tot taak de veiligheid van Nederland te waarborgen en strafbare feiten op te sporen. Het kabinet onderstreept hierbij de noodzaak tot rechtmatige toegang tot gegevens en communicatie. Daarnaast zijn overheden, bedrijven en burgers gebaat bij maximale veiligheid van de digitale systemen. Het kabinet onderschrijft het belang van sterke encryptie voor de veiligheid op internet, ter ondersteuning van de bescherming van de persoonlijke levenssfeer van burgers, voor vertrouwelijke communicatie van overheid en bedrijven , en voor de Nederlandse economie.

Derhalve is het kabinet van mening dat het op dit moment niet wenselijk is om beperkende wettelijke maatregelen te nemen ten aanzien van de ontwikkeling, de beschikbaarheid en het gebruik van encryptie binnen Nederland. In de internationale context zal Nederland deze conclusie en de afwegingen die daaraan

ten grondslag liggen uitdragen. Ten aanzien van het stimuleren van sterke encryptie zal de minister van Economische Zaken opvolging geven aan de strekking van het amendement (TK 2015-2016, 34300 XIII, nr.10) op de begroting van het ministerie van Economische Zaken.

Minister van Veiligheid en Justitie,

G.A. Van der Steur

Minister van Economische Zaken,

H.G.J. Kamp