Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

~~Stg. GEHEIM~~
RVI

Directie Analyse en Strategie

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

Contactpersoon

art. 10.2e

nota

Dreiging Russische Federatie via Kaspersky

Datum
13 februari 2018

Ons kenmerk
EV

Van
NCTV
Datum/eindparaaf

Aanleiding

In de media is berichtgeving verschenen dat de overheden van de VS en het VK waarschuwen voor het gebruik van Kaspersky of Russische software. Kaspersky zou samenwerken met de Russische overheid om via haar software heimelijk toegang te krijgen tot ICT systemen. Een dergelijke samenwerking tussen Kaspersky en de Russische overheid is een in potentie zeer ernstige bedreiging voor de nationale veiligheid. Een dergelijke samenwerking zou Nederlandse klanten van Kaspersky kwetsbaar kunnen maken voor cyberspionage en cybersabotage door Rusland. De Nederlands overheid en vitale infrastructuur zijn vrijwel volledig afhankelijk van ICT voor de continuïteit van de bedrijfsvoering .

art. 11 en 10.1b

Gevraagd besluit

U wordt gevraagd:

art. 11

Directie Analyse en Strategie

Datum
18 januari 2018

Ons kenmerk
EV

art. 11

Toelichting

Dreigingsappreciatie

art. 10.1b

Dreigingsanalyse Kaspersky Labs (NCTV open bronnen analyse)

Aanleiding voor de analyse is berichtgeving in media omtrent verdenkingen van onbehoorlijk handelen van de Russische antivirussoftwareontwikkelaar Kaspersky Labs. Dit mede in de context van bevindingen over de dreiging die uitgaat van statelijke actoren in het CyberSecurity Beeld Nederland en openbare jaarverslagen van de AIVD en MIVD. De analyse is gebaseerd op open bronnen. De conclusies van deze analyse zijn:

Conclusie 1: Vanwege de aard van een cybersecurity-bedrijf en haar producten en diensten kan misbruik een aantrekkelijk cybermiddel zijn voor een statelijke (of andere) actor. Of dit middel ook daadwerkelijk ingezet wordt, is afhankelijk van de intenties van de betreffende actor en de mogelijkheden voor misbruik.

Conclusie 2: Wanneer misbruik plaatsvindt van producten en diensten van AV-bedrijven, zoals Kaspersky, vormt dit een dreiging voor de Nationale Veiligheid door:

1. Aantasting van de cybersecurity van informatie en machines met als motief sabotage. Deze dreiging heeft de meeste impact.
2. Aantasting van de vertrouwelijkheid van informatie en machines met als motief spionage.
3. Ontwikkeling van geavanceerde aanvalstechnieken. Het motief is om op lange termijn aanvals- en verdedigingscapaciteit op te bouwen. Daadwerkelijk effect vindt pas plaats bij actieve inzet van de technieken.

Conclusie 3: Wat betreft de manifestatie van de geïdentificeerde dreigingen zijn verschillende scenario's voorstelbaar. Op dit moment is geen sluitend bewijs te vinden in open bronnen voor één of meerdere van de scenario's en kan er daarom geen uitsluitsel gegeven worden of Kaspersky op dit moment actief een dreiging vormt voor de Nationale Veiligheid. De dreiging van statelijke actoren in het digitale domein en de wetgeving met betrekking tot cryptografie en de samenwerking met de FSB moet beschouwd worden als een risico.

Scenario 3A: Het is waarschijnlijk dat Kaspersky door de Russische overheid gedwongen wordt om samen te werken, maar dat eigenlijk niet wil (scenario bewust-ongewild).
Scenario 3B: Het is waarschijnlijk dat Kaspersky geïnfiltreerd en gecompromitteerd is of wordt door een andere (dan de Russische) overheid (onbewust-ongewild).

Tot slot wordt in de analyse opgemerkt dat van andere Cybersecurity-bedrijven dezelfde dreiging kan uitgaan als die van Kaspersky en soortgelijke scenario's denkbaar zijn. Andere Cybersecurity-bedrijven hebben dezelfde middelen en kunnen ook door hun respectievelijke overheden in meer of mindere mate gedwongen worden tot samenwerking.

art. 10.1b

art. 10.1b

art. 11

art. 11

art. 10.1b

Geopolitieke consequenties

Kaspersky is een prominent Russisch bedrijf en met het opzeggen van het vertrouwen in Kaspersky en Russische ICT-bedrijven in het algemeen neemt Nederland een besluit met zowel politieke als economische consequenties. Daarom moet rekening worden gehouden met mogelijke politieke of economische represailles van Rusland tegen Nederlandse belangen.

Handelingsperspectief

Staken dienstverlening Kaspersky

Kaspersky is primair een leverancier van antivirus- en cybersecuritysoftware. Voor deze producten zijn wereldwijd alternatieven beschikbaar van andere leveranciers. Hoewel dit een ingrijpende ingreep is, is er handelingsperspectief door de dienstverlening door Kaspersky te staken en over te stappen op een alternatieve dienstverlener. [redacted]

art. 11

[redacted] Het staken van de dienstverlening behelst de volgende maatregelen:

1. **Bestaande dienstverlening staken**
   Opzeggen contracten en licenties en verwijderen software.

   [redacted]

   art. 11

2. **Toekomstige dienstverlening weren**

   [redacted]

   art. 11

3. **Communicatie mbt gebruik van Kaspersky / Russische software (afhankelijk van keuze voor reikwijdte) bij overheden, vitale**

Directie Analyse en Strategie

infrastructuur en bij bedrijven.

art. 11

Datum
18 januari 2018

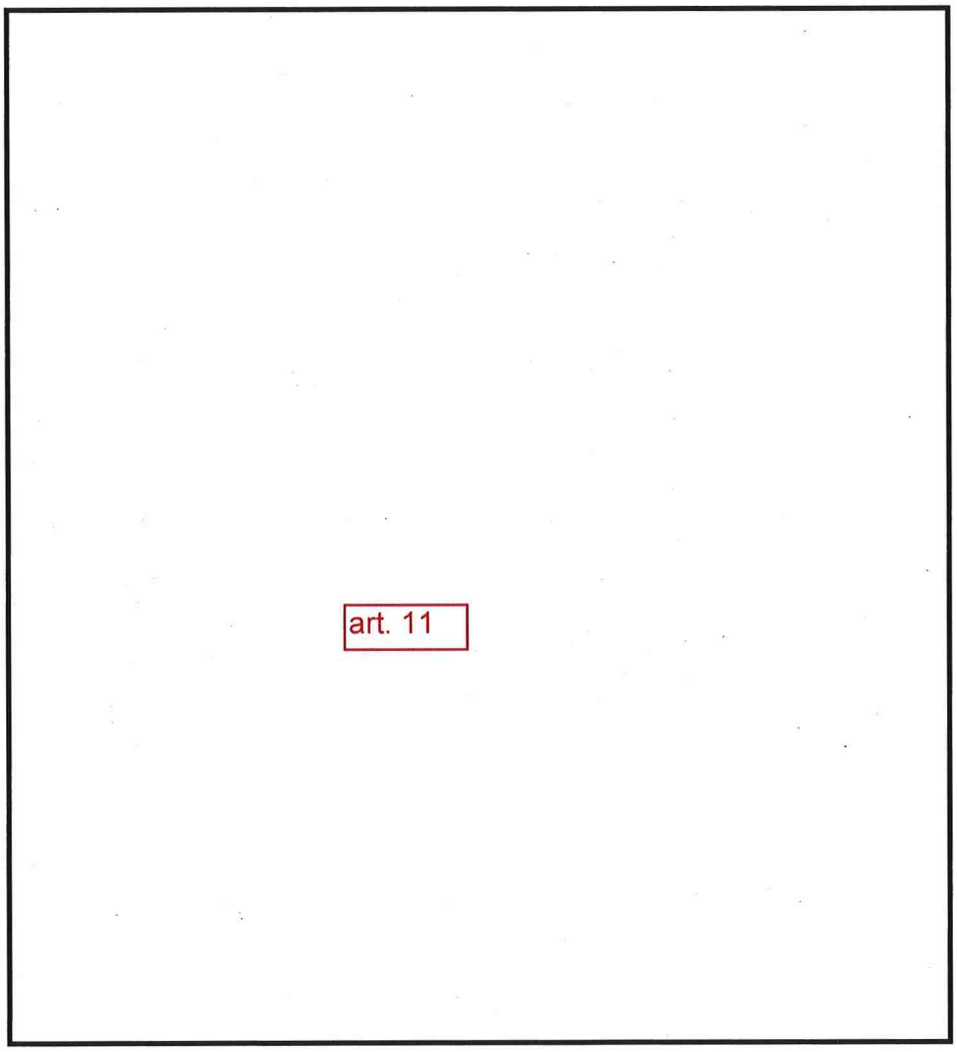
Ons kenmerk
EV

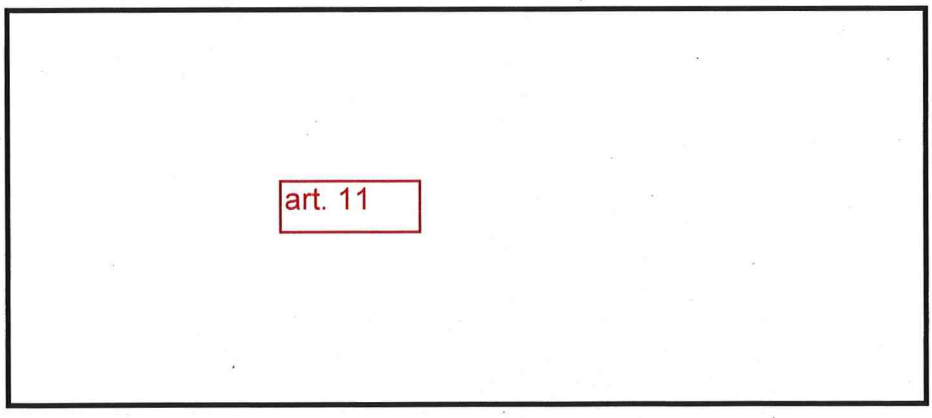
art. 11

Directie Analyse en Strategie

Datum
18 januari 2018

Ons kenmerk
EV





Directie Analyse en Strategie

Datum
18 januari 2018

Ons kenmerk
EV

art. 11

art. 11

art. 11

art. 11

Directie Analyse en Strategie

Datum
18 januari 2018

Ons kenmerk
EV

art. 11

art. 10.1b

Directie Analyse en Strategie

Datum
18 januari 2018

Ons kenmerk
EV