Ministerie van Economische Zaken
en Klimaat

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Tweede Kamer
der Staten-Generaal
Binnenhof 4
2513 AA DEN HAAG

Directoraat-generaal
Bedrijfsleven & Innovatie

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
F 070 378 6100 (algemeen)
www.rijksoverheid.nl/ezk

Ons kenmerk
DGBI / 19103104

Uw kenmerk
2019Z07442

Datum 29 mei 2019
Betreft Diefstal van bedrijfsvertrouwelijke gegevens bij ASML

Geachte Voorzitter,

Met deze brief reageer ik op het verzoek van het lid Van der Lee om in te gaan op de diefstal van bedrijfsvertrouwelijke gegevens bij het bedrijf ASML, waarover recent in de pers is bericht.
In deze brief zal ik eerst een overzicht geven van de feitelijke gebeurtenissen zoals die mij bekend zijn. Vervolgens zal ik een duiding hiervan geven en beschrijven welke acties het kabinet op dit punt onderneemt.

Algemeen

Zoals ook in diverse media is bericht, zijn in de loop van 2014 bij de Amerikaanse dochteronderneming ASML US Inc. bedrijfsvertrouwelijke gegevens door oud-werknemers ontvreemd en terechtgekomen bij een concurrerend bedrijf XTAL Inc. Beide bedrijven zijn gevestigd in San José, California. De betreffende ex-werknemers waren afkomstig van het bedrijf Brion technologies inc dat in 2007 door ASML is overgenomen en zijn later in dienst getreden bij XTAL. Zowel XTAL als Brion zijn actief in de ontwikkeling van geavanceerde software voor de lithografie industrie (zogenoemde *computational lithography*). De producten van Brion/ASML en XTAL waar het hier over gaat, worden gebruikt door afnemers actief in de productie van halfgeleiders. Uit de in de VS gevoerde rechtszaken komt naar voren dat bedrijfsvertrouwelijke gegevens van ASML zijn gebruikt in de producten die XTAL aanbood aan zijn klanten en dat deze bedrijfsvertrouwelijke gegevens via de betreffende ex-werknemers van ASML in handen van XTAL zijn gekomen. Door een Amerikaanse jury is in 2018 vastgesteld dat door XTAL inbreuk is gemaakt op de bedrijfsgeheimen van ASML, hetgeen er recent toe heeft geleid dat XTAL in een finale beslissing is veroordeeld tot betaling van een bedrag van 845 miljoen dollar. Dit bedrag is gebaseerd op ongerechtvaardigde verrijking (vanwege vermeden R&D kosten) en *punitive damages*. XTAL is inmiddels in staat van faillissement geraakt, welke procedure thans wordt afgewikkeld. Dientengevolge zal dit bedrag waarschijnlijk niet inbaar zijn. Daarnaast zijn partijen een schikking overeengekomen (goedgekeurd door de Amerikaanse rechter) op grond waarvan XTAL en zijn werknemers gedurende drie jaar niet in dezelfde bedrijfstak werkzaam mogen zijn, alle octrooien van XTAL worden overgedragen aan ASML en harddisks met source codes worden overgedragen.

Het bedrijf XTAL en de betrokkenheid van de Chinese overheid

In de pers is veel aandacht besteed aan de status van het bedrijf XTAL en de betrokkenheid van de Chinese overheid. Wat wij hierover weten is het volgende. Volgens informatie die tot voor kort op de website van XTAL beschikbaar was, zijn er twee investeerders betrokken bij het bedrijf: Finest Sino, (een dochterbedrijf van de China Oriental Group Company ltd (COGCL; een in Hong Kong geregistreerde vennootschap) en vanaf 2016 Samsung Venture Investment Cooperation (SVIC; een Koreaanse investeringsfirma). Oprichters en leidinggevenden van XTAL zijn technici van Chinese afkomst, met deels de Amerikaanse nationaliteit, die in de VS hebben gestudeerd en/of werkzaam zijn geweest, onder meer bij ASML of haar dochter Brion. Een aantal ex-medewerkers van ASML komt ook voor in de juridische procedures die betrekking hebben op de schending van bedrijfsgeheimen.

Door ASML is in persberichten aangegeven dat de informatie die op onrechtmatige wijze in handen is gekomen van XTAL, is gebruikt voor commerciële doeleinden. Meer in het bijzonder is deze informatie gebruikt bij de ontwikkeling van producten die zijn aangeboden aan afnemers, waaronder ook een klant van ASML. Door ASML is ook aangegeven geen aanwijzingen te hebben van betrokkenheid van de Chinese overheid bij dit concrete geval.

Welke bedrijfsvertrouwelijke gegevens zijn ontvreemd en hoe belangrijk zijn deze?

De ontvreemde gegevens hebben betrekking op software die door klanten van ASML wordt gebruikt voor de verbetering van het proces van het vervaardigen van halfgeleiders met behulp van de ASML machines. Volgens informatie van ASML representeren deze activiteiten minder dan 1% van haar inkomsten. Dat neemt niet weg dat de onrechtmatig verkregen informatie een belangrijke waarde vertegenwoordigt. Dat blijkt uit de verplichting tot het betalen van het bedrag van 845 miljoen dollar, waartoe XTAL door de Amerikaanse rechter is veroordeeld. Dit bedrag is voornamelijk gebaseerd op het voordeel dat XTAL heeft genoten doordat het R&D kosten heeft weten te vermijden en punative damages. Het belang voor een bedrijf als ASML is erin gelegen deze kennis goed te beschermen, zodat gemaakte investeringen kunnen worden terugverdiend en free rider gedrag wordt tegengegaan.

Duiding van de gebeurtenissen in de VS

Schending van bedrijfsgeheimen door ex-werknemers is een kwalijke, maar helaas veel voorkomende praktijk, die slecht is voor het ondernemingsklimaat en niet bevorderlijk is voor onze welvaart. Uit de afwikkeling van deze zaak blijkt dat als gevolg van de door ASML getroffen maatregelen het door de betrokken ex-werknemers en het bedrijf XTAL genoten voordeel inmiddels is tenietgedaan. Potentieel klantenverlies is voorkomen, ASML heeft de octrooien van XTAL verworven en XTAL en zijn medewerkers mogen voorlopig niet langer op hetzelfde terrein actief zijn. Daarmee is het voorval ook een goed voorbeeld dat het noodzakelijk en mogelijk is voor innoverende bedrijven om afschrikwekkende maatregelen te treffen wanneer wordt geconstateerd dat bedrijfsgeheimen zijn geschonden.

Economische spionage

Ik heb geen aanwijzingen dat er in casu sprake is geweest van directe betrokkenheid van een buitenlandse overheid. Er zijn wel overeenkomsten te zien met bekende spionagedoelwitten en -werkwijzen. Ik verwijs in dit verband naar het jaarverslag van de AIVD.

Welke maatregelen treft het kabinet?

Vooropgesteld moet worden dat het onderhavige geval volledig heeft plaatsgevonden in de Verenigde Staten en de maatregelen die ASML heeft getroffen ook volledig daar hebben plaatsgevonden. Het Amerikaanse rechtssysteem biedt daarvoor ook goede mogelijkheden.
Dat neemt niet weg dat schending van bedrijfsgeheimen ook hier voor kan komen en het noodzakelijk is om daartegen maatregelen te treffen. De primaire verantwoordelijkheid voor het treffen van maatregelen ligt bij bedrijven zelf. De overheid stelt hen daartoe in staat, onder meer door regelgeving, handhaving, rechtspraak en voorlichting.

Belangrijk daarbij is de wetgeving op het gebied van intellectuele-eigendomsbescherming en bescherming van bedrijfsgeheimen. Op 23 oktober 2018 is de Wet bescherming bedrijfsgeheimen in werking getreden, waaraan ondernemers bescherming kunnen ontlenen als hun bedrijfsgeheim onrechtmatig is verkregen, gebruikt of openbaar gemaakt, ook als dit door een ex-werknemer is gebeurd. Daarnaast kan bescherming ook worden verkregen op basis van het arbeidsrecht of algemene contractenrecht als een ex-werknemer bijv. zijn geheimhoudingsbeding heeft geschonden, of op basis van het algemene onrechtmatigedaadsrecht. Er kan bovendien onder omstandigheden een beroep worden gedaan op bescherming tegen een inbreuk op een octrooirecht of op een chipsrecht op basis van de Wet bescherming oorspronkelijke topografieën van halfgeleiderproducten.

Daarnaast heeft de overheid de verantwoordelijkheid voor het creëren van awareness voor risico's en het bieden van een handelingsperspectief.

Directoraat-generaal
Bedrijfsleven & Innovatie

Ons kenmerk
DGBI / 19103104

Door de Rijksdienst voor Ondernemend Nederland wordt voorlichting gegeven aan bedrijven over hoe zij hun kennis het beste kunnen beschermen en hoe zich kunnen wapenen tegen misbruik door derden. Daarnaast is het Digital Trust Center opgericht, dat niet-vitale ondernemers helpt veilig om te gaan met digitale gegevens. Ook is er het Nationaal Cyber Security Centrum (NCSC) als centrale informatieknooppunt en expertisecentrum op het gebied van cybersecurity voor de Rijksoverheid en organisaties binnen de vitale infrastructuur. Specifiek met betrekking tot spionage kunnen bedrijven hun kwetsbaarheden in kaart brengen met de door de het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ontwikkelde Kwetsbaarheidsanalyse Spionage. Voorts verwijs ik in dit verband naar de brief over statelijke dreigingen die de minister van Justitie en Veiligheid u onlangs heeft gestuurd.[1]

Eric Wiebes
Minister van Economische Zaken en Klimaat

[1] Brief van de Minister van Justitie en Veiligheid over Tegengaan statelijke dreigingen 18 april 2019: https://www.rijksoverheid.nl/documenten/kamerstukken/2019/04/18/tk-tegengaan-statelijke-dreigingen