Aanbeveling

11.04.2017 • *Leestijd 4 minuten*

Er wordt al jaren over gespeculeerd hoe Europese bedrijven ondanks strenge regelgeving spionagesoftware weten te verkopen aan dictaturen. Al Jazeera vond eindelijk het bewijs. Een warme aanbeveling voor een heel goede documentaire.

Eindelijk bewijs: zo komen dictators aan spionagesoftwar e

Correspondent
Veiligheidsindustrie

Dimitri **TOKMETZIS**

Still uit de documentaire Spy Merchants van Al Jazeera.

Het was de afgelopen maanden een flinke frustratie. Met een groep Europese journalisten onderzochten we de export van spionagesoftware en -apparatuur naar dictatoriale landen. Met deze spullen kunnen inlichtingendiensten bijvoorbeeld het internetverkeer van grote delen van de bevolking onderscheppen en analyseren. Telefoons kunnen worden afgeluisterd, computers worden gehackt. Vroeger was dit voor veel landen vrij moeilijk: technisch lastig en erg kostbaar. Tegenwoordig kunnen ze de soft- en hardware hiervoor kant-en-klaar kopen bij bedrijven, en dat voor een redelijke prijs.

Het gebruik van dit soort soft- en hardware leidt tot grote problemen voor activisten, journalisten en oppositie van dictatoriale regimes. Op basis van afgeluisterde berichten en gehackte computers worden mensen gearresteerd en wordt er soms nooit meer iets van ze vernomen. Kort geleden vroeg ik hier nog aandacht voor Ahmed Mansoor, een prominente mensenrechtenactivist in de Verenigde Arabische Emiraten. Op zijn computers is nu al een aantal keer spionagesoftware

gevonden en drie weken geleden werd hij weer gearresteerd. Er is nog niets over zijn lot bekend.

De vraag naar spionagetools neemt toe

Zeker na de Arabische Lente nam de vraag van dictatoriale regimes naar dit soort software sterk toe. Als reactie hierop gelden sinds 31 december 2014 strengere regels voor de export van dit soort software vanuit de Europese Unie.

Met onze onderzoeksgroep wilden we zien of deze regulering goed werkt. Als een bedrijf spionagesoftware wil exporteren, moet het een vergunning aanvragen. Als een overheid de kans op misbruik te groot acht, kan de vergunning geweigerd worden.

We vonden al snel een paar vreemde dingen. Ten eerste is de ene lidstaat strenger dan de andere in het verlenen van vergunningen. Vanuit Italië is het bijvoorbeeld makkelijker exporteren dan vanuit Nederland. De regels zijn hetzelfde, maar de interpretatie verschilt aanzienlijk. Dat biedt ruimte aan bedrijven om de makkelijkste exportroute te vinden.

Ten tweede zagen we dat veel Europese bedrijven kantoren hebben buiten de Europese Unie. Zo hebben minstens 42 Europese bedrijven een kantoor in de Verenigde Arabische Emiraten. Er is geen zicht op wat ze daar precies doen.

Maar er waren twee vermoedens die we maar niet rondkregen, vandaar onze frustratie.

Het eerste vermoeden was dat Europese bedrijven daadwerkelijk gebruikmaken van bedrijven buiten de Europese Unie, bijvoorbeeld een dochteronderneming of een tussenpersoon, om spionagesoftware aan dubieuze regimes te verkopen.

Ons tweede vermoeden was dat bedrijven simpelweg liegen over wat ze verkopen. Als ze zeggen dat ze bijvoorbeeld een IMSI-catcher verkopen, moeten ze een vergunning aanvragen. Maar als ze die IMSI-catcher een wifi-router noemen die voor testdoeleinden wordt gebruikt, dan is zo'n vergunning niet nodig.

De enige manier om erachter te komen of deze vermoedens klopten, was om *insiders* in de industrie aan het praten te krijgen. Maar zij hielden hun kaken op elkaar, hoe vaak en indringend we ze ook benaderden.

De oplossing: *undercover* journalistiek

Het is daarom goed om te zien dat het nieuwsorganisatie Al Jazeera wel gelukt is deze vermoedens bevestigd te krijgen. Het onderzoeksteam heeft een indrukwekkende undercoveroperatie uitgevoerd en maakte er een documentaire over.

Een spijtoptant uit de industrie, ene 'James,' deed zich vier maanden voor als tussenpersoon voor drie verschillende partijen: de overheid van Zuid-Soedan, waar een ernstig conflict woedt, de veiligheidsdiensten van Iran, dat op verschillende sanctielijsten staat, en tot slot voor een partij wiens identiteit hij niet aan de leveranciers wilde onthullen.

Dat kon een privaat bedrijf zijn, maar ook een criminele of terroristische organisatie.

Voor iedere 'klant' vond James een bedrijf dat spionagesoftware of -apparatuur wilde leveren.

Een bevriend Turks bedrijf kon wel iets regelen

De eerste die toehapte was Area. Dat Italiaanse bedrijf was bereid om een IMSI-catcher te leveren aan Zuid-Soedan. Daarvoor zou het bedrijf geen exportlicentie krijgen, maar CEO Marco Braccioli wist wel een oplossing: een bevriend bedrijf in Turkije zou de deal kunnen sluiten. De Turkse contactpersoon, Alper Tuson, kon via zijn contacten bij inlichtingendienst MIT toestemming krijgen om binnen vier weken het apparaat en de software te exporteren. En belangrijk: Tuson zou gewoon liegen over de aard van de software. Hij zou op de papieren invullen dat het ging om telecommunicatieapparatuur.

Het tweede bedrijf dat wel zaken wilde doen, was iPS, eveneens een Italiaans bedrijf. Dat bood aan om voor twintig miljoen euro apparatuur en software te installeren waarmee de Iraanse geheime dienst internetverkeer kon aftappen. Goed, de export van dit soort goederen naar Iran is verboden, maar ze zouden de apparatuur en software leveren via RESI, een bedrijf dat verkeersmanagementsystemen maakt. Geen

enkel probleem.

nd James een Chinees bedrijf, Semptian, dat tien IMSI-catchers te leveren, zonder dat ze de klanten waren. Dat konden criminelen zijn, terroristen, of bedrijven die concurrenten wilden afluisteren. De salesmanagers stelden voor alles via een brievenbusfirma te laten lopen en net te doen alsof er wifi-routers werden geëxporteerd. De CEO van Semptian vroeg nog of de betaling - twee tot drie ton per apparaat - dit jaar geregeld kon worden omdat hij nog een verkooptarget te halen had dit jaar.

De documentaire van Al Jazeera legt feilloos bloot hoe schaamteloos deze bedrijven te werk gaan. De exportregels zijn niet meer dan drempels waar ze makkelijk omheen manoeuvreren omdat blijkbaar niemand de naleving echt controleert.

Maar, zoals een van de advocaten aan het einde terecht opmerkt, dit verhaal gaat niet over alleen het omzeilen van een paar regeltjes. Dit verhaal gaat over medeplichtigheid aan onrechtmatige gevangenschap, marteling en misdrijven van dictatoriale regimes.

Kijken dus.

Meer lezen over de surveillance-industrie?

met links, infocards, eventuele videos en ledenbijdragen, ga naar: https://decorrespondent.nl/6534/eindelijk-bewijs-zo-komen-dictators-aan-spionagesoftware/1620137133648-7e63e08e

De Correspondent is een dagelijks, advertentievrij medium met als belangrijkste doelstelling om de wereld van meer context te voorzien. Door het nieuws in een breder perspectief of in een ander licht te plaatsen, willen wij het begrip 'actualiteit' herdefiniëren: niet om je aandacht te trekken, maar om je inzicht te bieden in hoe de wereld werkt.

decorrespondent.nl

Alle verhalen lezen? Dat kan voor €6 per maand op: decorrespondent.nl