DigiTask, Duitse leverancier van onveilige en onbetrouwbare spyware (profiel)

Het Duitse bedrijf DigiTask was een van de eerste bedrijven die software ontwikkelde om computers en telefoons te hacken en te doorzoeken. De Duitse overheid gebruikte sinds 2007 de spyware van DigiTask. Het bedrijf leverde haar spyware ook aan Nederland.

In 2011 werd de spyware onderzocht door het hackerscollectief CCC en de Duitse landelijke databeschermingsautoriteiten en die van verschillende deelstaten, waaronder Beieren. Het is een van de weinige keren dat spyware uitgebreid is onderzocht door derden en niet door de leverancier of de overheid die de spyware gebruikt.

Uit deze onderzoeken blijkt dat de politie weinig inzicht heeft in de werking van de tools van DigiTask en de wijze waarop gegevens verkregen worden. De leverancier, en mogelijk derden, kunnen toegang krijgen tot de spyware, gegevensdragers van verdachten en servers en kunnen gegevens, toevoegen of wijzigen. De onderzoeken leggen de tekortkomingen bloot die inherent zijn aan alle commerciële spyware. De betrouwbaarheid van het verkregen bewijsmateriaal is bij alle commerciële spyware in het geding.

Volgens de Duitse overheid wordt spyware, waaronder die van DigiTask, ingezet bij de bestrijding van terrorisme en zware georganiseerde criminaliteit. Het is echter moeilijk om deze claim te beoordelen. De Duitse overheid publiceert, net als andere landen, nauwelijks gegevens over de inzet van spyware, zoals het aantal en het type zaken waarin spyware is ingezet, het aantal zaken waarin dit tot een veroordeling heeft geleid, en tot welke straf.

Mediaberichtgeving, rapporten van databeschermingsautoriteiten en andere openbare bronnen duiden erop dat de spyware van DigiTask nauwelijks is ingezet in onderzoek naar verdachten van terrorisme, maar vooral bij

onderzoeken naar minder zware vergrijpen. Het is onduidelijk in hoeveel zaken dit daadwerkelijk tot een veroordeling heeft geleid.
Ook andere landen, waaronder Zwitserland, België en Nederland, hebben de tools van het Duitse bedrijf aangeschaft. Toenmalig Minister van Veiligheid en Justitie Opstelten verklaarde in 2011 dat de Nederlandse politie de spyware van DigiTask had aangekocht, nadat dit eerder door het Duitse bedrijf zelf naar buiten was gebracht. Het lijkt erop dat de Nederlandse politie de spyware in ieder geval tot 2014 is blijven gebruiken.

In de loop der jaren heeft DigiTask miljoenen euro verdiend aan de verkoop van spyware aan niet alleen de Duitse overheid, maar ook buitenlandse overheden. Dit valt ten minste opmerkelijk te noemen. Het bedrijf leverde onveilige en onbetrouwbare apparatuur. Bovendien heeft het bedrijf een verleden van corruptie en een veroordeling vanwege het betalen van steekpenningen.

Van Reuter Leiterplatten naar DigiTask

Digi Task GmbH Gesellschaft für besondere Telekommunikationssysteme wordt in 2000 opgericht in Haiger in de deelstaat Hessen. De voorloper van het bedrijf is Reuter Leiterplatten GmbH, dat vanaf 1986 samen met Reuter Electronic afluisterapparatuur voor de Duitse opsporings- en inlichtingendiensten ontwikkelde. DigiTask is zeer nauw verbonden met het bedrijf Reuter Electronic GmbH van eigenaar Hans-Hermann Reuter.

DigiTask is een van de eerste bedrijven die software aanbiedt om computers en telefoons te hacken en binnen te dringen. De software is betrekkelijk goedkoop en eenvoudig te gebruiken, in vergelijking met bijvoorbeeld FinFisher van Gamma Group en DaVinci (Da Vinci) en Galileo RCS (Remote Control System) van Hacking Team.

DigiTask begeeft zich op de internationale markt. Zo presenteert het bedrijf zich op de ISS World beurzen. ISS-World (Intelligence Support Systems) is een handelsbeurs voor afluister- en surveillance-apparatuur. Naast bedrijven zijn medewerkers van legers, politie en inlichtingendiensten uit verschillende landen in het Midden-Oosten aanwezig. Ook het Nederlandse Fox-IT is op de

beurzen te vinden, net als ambtenaren van Nederlandse ministeries, het Nederlands Forensisch Instituut en politiefunctionarissen van de toenmalige KLPD (Korps landelijke politiediensten, nu de landelijke eenheid).

DigiTask presenteert haar producten op de ISS World beurzen in 2008 en 2009 in Dubai en van 2008 tot en met 2010 en 2012 in Praag. In presentaties uit oktober 2008 en juni 2009 stelt Dr. Michael Thomas dat DigiTask al jaren actief is op de surveillance markt en speciale oplossingen voor afluisteroperaties ontwikkelt.

Het bedrijf beweert dat het marktleider is in Duitsland. "*Digitask has overall experience of many years in LI systems, is market leader for LI in Germany and is privately owned and independent (LI Lawful Interception)*", aldus zijn presentatie op ISS World in 2008 over 'Remote Forensic Software'.

Dat DigiTask marktleider in Duitsland is wordt opnieuw onderstreept op de ISS World beurs in Praag in juni 2009 door twee andere medewerkers van het bedrijf: Tobias Hain tijdens de presentatie "Challenges in Intercepting WiFi" en Thomas Kröckel bij "Future Challenges in the Lawful Interception of IP based Telecommunication."

DigiTask in Beieren

In 2008 wordt bekend dat de Beierse overheid gebruik maakt van de spyware van DigiTask. De Duitse Piratenpartij maakt via WikiLeaks twee documenten openbaar die wijzen op de ontwikkeling/aanschaf van interceptie programmatuur door de Beierse overheid.

Een document is een brief van het Beierse Ministerie van Justitie aan het Openbaar Ministerie in München over de kosten van de aanschaf en welke instantie de rekening gaat betalen.

In de brief wordt gesproken over de aanschaf van software van de firma DigiTask waarmee VoIP-gesprekken (Voice over IP) kunnen worden afgetapt. De spyware wordt direct of via een e-mail geïnstalleerd op de computers van verdachten om programma's zoals het destijds populaire

Skype af te luisteren en beveiligde communicatie van verdachten te ontsleutelen. Dit gebeurt bijvoorbeeld met een 'Skype Capture Unit', die gesprekken real time kan streamen naar de Duitse autoriteiten. De ontsleutelde bestanden worden verstuurd naar een server die tegelijkertijd tien gesprekken via Skype kan opnemen. Het Skype-gesprek zelf wordt niet onderbroken. Het gaat om een zogenaamd 'man in the middle' aanval die moeilijk te ontdekken is voor de persoon waarbij de tool wordt gebruikt.

Het andere document betreft een aanbod van DigiTask van 4 september 2007 om software te leveren waarmee Skype-gesprekken van verdachten kunnen worden afgeluisterd. Het bedrijf rekent 3.500,00 euro per maand voor het huren van de software. Eenmalig wordt 2500 euro in rekening gebracht voor installatie en verwijderingskosten van de computer van de verdachte. Voor datzelfde bedrag decodeert DigiTask de communicatie van de verdachte met zijn bank, online winkels, web-mail, e-mail, chatprogramma's, andere internetactiviteiten en programma's op de verdachte computer. Volgens het document kost een abonnement voor de tool 200.000 euro per jaar.

Het is een gevoelig onderwerp voor de Duitse autoriteiten. Op 11 september 2008 doet de politie een inval op het privéadres van een van de woordvoerders van de Piratenpartij en neemt computers in beslag. De overheid is op zoek naar de anonieme bron die de twee documenten aan de Piratenpartij heeft gelekt. De Duitse overheid wil niet dat openbaar wordt dat de politie spyware of - zoals de tools in Duitsland worden genoemd - Staatstrojaner (overheidsmalware) gebruikt.

De Duitse wetgeving biedt op dat moment wel enige ruimte voor het gebruik van spyware door de overheid. Het Duitse verleden en de sterk ontwikkelde privacy cultuur in het land zorgen echter voor een stevige oppositie. Door de spyware als Staatstrojaner te labelen en te spreken over 'Stasi 2.0' domineren de tegenstanders van de inzet van spyware lange tijd het publieke debat in Duitsland.

Daarnaast is het zeer opmerkelijk dat de Duitse overheid producten van DigiTask koopt, vanwege het dubieuze verleden van het bedrijf.

Steekpenningen

De voorganger van DigiTask was Reuter Leiterplatten. Eind vorige eeuw werd de directeur van dit bedrijf, Hans-Hermann Reuter, tevens bedrijfsleider van Reuter Electronic, gearresteerd in verband met het (gedurende een periode van tien jaar) betalen van steekpenningen aan ambtenaren van de douane. In 2002 werd Reuter wegens corruptie veroordeeld tot 21 maanden gevangenisstraf en een boete van 1,5 miljoen euro. Volgens het tijdschrift *Focus* heeft Reuter door het betalen van steekpenningen 50 miljoen Duitse Mark aan opdrachten voor het bedrijf binnengehaald.

Reuter Leiterplatten was volgens ZDF en het tijdschrift *Wirtschaftswoche* in de jaren negentig ook bereid om illegaal afluisterapparatuur te leveren aan Deutsche Telekom voor het afluisteren van medewerkers van het bedrijf. Uit interne documenten van Deutsche Telecom blijkt dat 120 gesprekken van vier telefoonnummers werden afgeluisterd. De drie afgeluisterde personen werden in december 1996 verdacht van een mogelijke hackaanval op de systemen van Deutsche Telecom. Het bedrijf luisterde de medewerkers af zonder gerechtelijk bevel. Toen het toenmalige Bundesministerium für Post und Telekommunikation hiervan op de hoogte werd gesteld bestempelde het de operatie als illegaal.

Na de arrestatie van Reuter in 1999 en de naamsverandering van Reuter Leiterplatten in DigiTask in 2000 werd – in overleg met het Ministerie van Justitie - Deloitte Deutschland formeel verantwoordelijk voor het bedrijf, hetgeen het tot 2006 zou blijven. Deloitte zegt niet actief betrokken te zijn geweest bij de bedrijfsvoering. Het heeft naar alle waarschijnlijkheid alleen het bedrijf draaiende gehouden in verband met lopende opdrachten van de Duitse overheid. Voor de Duitse overheid was het van belang dat DigiTask niet kon omvallen.

Wanneer in 2008 bekend wordt dat de Duitse overheid spyware van DigiTask heeft aangekocht claimen de autoriteiten dat Hans-Hermann Reuter na zijn straf te hebben uitgezeten geen betrokkenheid meer heeft met het bedrijf. Het is echter de vraag of dit daadwerkelijk zo is. In 2006 kwam het bedrijf namelijk in handen van Reuter en kwamen de bedrijfseigendommen op zijn naam.

Ook is Reuter in 2008 nog steeds eigenaar van Reuter Electronic, dat nauw samenwerkt met DigiTask. Daarnaast bevestigt de advocaat van DigiTask in *Frankfurter Rundschau* dat de bedrijfsleiding van DigiTask in handen is van de echtgenote van Reuter. Reuter zelf zou volgens zijn advocaat echter niets met het bedrijf te maken hebben. De dagelijkse leiding van het bedrijf zou in handen zijn van Achim Pulverich. Hoe de verhouding tussen Hans-Hermann Reuter, Reuter Electronic en DigiTask precies is geregeld maakt het bedrijf niet openbaar.

Spyware ter discussie in rechtszaak

In 2011 laait het debat over het gebruik van spyware in opsporingsonderzoeken in Duitsland op. Aanleiding is een rechtszaak tegen een verdachte van de handel in farmaceutische producten. Tijdens de rechtszaak blijkt dat op de computer van de verdachte spyware is geïnstalleerd. Later zal blijken dat het gaat om spyware van DigiTask.

De Duitse rechter beoordeelt de inzet van de spyware deels als rechtmatig. Volgens de rechter is de monitoring van de Skype-gesprekken geoorloofd en in overeenstemming met de op dat moment geldende Duitse wetgeving. In de toestemming voor het gebruik van de spyware was in april 2009 toestemming gegeven voor het drie maanden afluisteren van audio en geschreven communicatie.

Het constant nemen van screenshots wordt door de rechter echter als onrechtmatig beoordeeld. De spyware op de computer van de cliënt van advocaat Patrick Schladt stuurde elke dertig seconden een screenshot naar een server van de politie. De screenshots waren afbeeldingen van alle handelingen op de computer van de verdachte zoals het gebruik van e-mail,

internet browsen en andere handelingen. Voor deze laatste inbreuk is volgens de Duitse rechter geen rechtsgrond.

Volgens advocaat Schladt is de spyware waarschijnlijk in de lente van 2009 op de luchthaven van München bij de douanecontrole op de computer van zijn cliënt geïnstalleerd. Nadat de verdachte is aangeklaagd bestuderen Schladt en zijn cliënt het dossier en vermoeden dat het digitale bewijs is verkregen door de inzet van spyware. Spyware die misschien nog steeds op de laptop van de verdachte aanwezig is.

Volgens de Duitse wetgeving is inzet van spyware alleen toegestaan bij verdenking van terrorisme of ernstige misdrijven. Hiervan is in deze zaak echter geen sprake. De cliënt van Schladt wordt verdacht van de handel in farmaceutische producten. Hij werkt voor een bedrijf dat handelt in producten die in Duitsland legaal zijn, maar buiten Duitsland deels niet.

Voor advocaat Schladt is daarmee de kous niet af. Het gaat hem niet alleen om de rechtmatigheid van de inzet van de spyware, maar zeker om de vraag hoe de spyware precies functioneert. Hij benadert daarom de Duits Chaos Computer Club (CCC), een collectief van ethische hackers, om nader onderzoek te doen naar het functioneren van de spyware.

Vernietigend CCC-rapport

De spyware die de CCC onderzoekt wordt door de Duitse overheid in het algemeen aangeduid als Quellen-TKÜ: bron telecommunicatie surveillance. In Duitsland worden twee andere namen veelvuldig gebruikt voor de door de CCC onderzochte spyware: Ozapftis en R2D2. Ozapftis is een verwijzing naar O'zapft is!, de traditie van het aanbreken van het eerste biervat door de burgemeester van München tijdens het Oktoberfeest. R2D2 is een verwijzing naar een digitale code van de spyware die de onderzoekers bij de analyse hebben gevonden, maar ook een verwijzing naar de ‘robot’ R2-D2 in Star Wars.

De CCC publiceert haar analyse op 8 oktober 2011. De onderzoekers concluderen veel tekortkomingen in de tool. Zij bevestigen de uitspraak van

de Beierse rechter dat de tool op de computer van de verdachte veel meer kan dan wettelijk is toegestaan in Duitsland. Met de spyware kunnen niet alleen Skypegesprekken worden afgeluisterd en screenshots worden gemaakt, hetgeen volgens de rechtbank is toegestaan. Er kunnen ook bestanden en programma's op de computer van de verdachte worden gemanipuleerd, vernietigd of toegevoegd.

De tool is dus niet alleen gericht op het afluisteren van de communicatie via een gegevensdrager, maar kan de computer of laptop in zijn geheel overnemen. Dit maakt manipulatie mogelijk, zoals het verwijderen en toevoegen van data op de computer van de verdachte, en – omdat de spyware ook toetsaanslagen registreert - het wijzigen van wachtwoorden. Dit is mogelijk omdat de tool op afstand bestuurd kan worden. Deze zogenaamde 'remote control' is mogelijk door een ingebouwde 'backdoor': een mogelijkheid die veel spyware heeft om een bepaalde functionaliteit van de tool te veranderen en uit te breiden.

Niet alleen de politie en de producent kunnen de spyware op afstand besturen. De CCC toont aan dat ook derden de computer van de verdachte kunnen overnemen, omdat de beveiliging van de backdoor niet op orde is en de verzamelde data niet versleuteld over het internet worden verzonden. Iedereen kan deze data dus in principe inzien.

Veel spyware communiceren met een server elders om zo direct de afgeluisterde data te verzamelen. Door de slechte beveiliging kan de tool door derden worden overgenomen en kunnen derden zelfs vervalste informatie naar de server van de autoriteiten sturen. Dit wordt veroorzaakt door het ontbreken van een authenticatiemechanisme in de tool: door de tool wordt niet vastgesteld met wie met de tool communiceert en door de tool verstuurde gegevens worden ook niet op echtheid gecontroleerd.

Tot slot stelt de CCC vast dat de server waarmee de spyware op de laptop van de verdachte mee communiceert, waarschijnlijk niet in Duitsland maar in de Verenigde Staten staat. De CCC baseert zich hierbij op het IP-adres van de server. De politie heeft dit waarschijnlijk zo ingericht om ontdekking van de tool te voorkomen. Communicatie van het besturingssysteem op de laptop, in dit geval Windows, of andere software met de Verenigde Staten wordt door de afgeluisterde persoon als minder verdacht beschouwd dan

communicatie met een server in Duitsland. Het bewaren van informatie over een verdachte op een buitenlandse server roept echter juridische vragen en vragen met betrekking tot de beveiligingsvragen, zoals in welk datacentrum de server staat en wie daar fysieke toegang toe heeft.

De CCC concludeert in haar onderzoek dat de tool die het heeft onderzocht afkomstig is van DigiTask. DigiTask verdedigt zich tegen de kritiek door te stellen dat de CCC een oude versie van de spyware heeft onderzocht: het zou gaan om een testversie of een prototype. De claim van DigiTask is bevreemdend, omdat de CCC stelt meerdere versies van de DigiTask tool te hebben onderzocht. En omdat het zou betekenen dat een onveilige testversie is gebruikt bij een opsporingsonderzoek.

De CCC heeft de herkomst van de andere onderzochte versies niet bekend gemaakt. Het gaat mogelijk om websites als VirusTotal en de databases van antivirus bedrijven, aangezien de spyware van DigiTask ook door verschillende antivirusprogramma's is ontdekt en geneutraliseerd. Delen van de spyware zijn zo in handen gekomen van deze bedrijven.

Het onderzoek van de CCC roept vragen op over de veiligheid van de inzet en de betrouwbaarheid van de verkregen informatie. Het belang van het CCC-onderzoek is niet alleen groot voor de situatie rond DigiTask, maar ook voor andere spyware. Het is namelijk de eerste keer dat spyware, of een deel van spyware, uitgebreid is onderzocht door derden en niet door de overheid of de bedrijven zelf.

Het onderzoek legt de vinger op de zere plek die bij alle spyware speelt. De politie heeft weinig inzicht in de werking van de tool en wijze waarop gegevens verkregen worden. De leverancier, en mogelijk, derden kunnen toegang krijgen en gegevens toevoegen of wijzigen. De betrouwbaarheid van door middel van spyware verkregen bewijsmateriaal is dus in het geding.

Een paar jaar later laat het Canadese Citizen Lab zien dat zij de communicatie tussen spyware en een server kan traceren en zo ontdekken welke computers en smartphones door overheidsinstanties zijn gehackt met tools als FinFisher (Gamma Group), Pegasus (NSO Group) of RCS (Hacking Team). Deze communicatie is natuurlijk de eerste stap bij de mogelijke onderschepping en manipulatie van die communicatie en daarmee bewijsmateriaal.

Onderzoek door Duitse databeschermingsautoriteiten

Het Duitse Ministerie van Binnenlandse Zaken en de politiediensten geven geen gedetailleerd commentaar op de bevindingen van de CCC en stellen geen nader onderzoek in. Verschillende databeschermingsautoriteiten, waaronder de landelijke en die van de deelstaat Beieren, doen wel onderzoek en zijn kritisch over het functioneren van de DigiTask spyware. Ze stellen fundamentele vragen bij de betrouwbaarheid van verkregen gegevens en bewijsmateriaal.

Het Beierse onderzoek is even kritisch als dat van de CCC, hoewel de databeschermingsautoriteit geen toegang krijgt tot de broncode van de DigiTask tool. Toegang tot de broncode is noodzakelijk om inzicht te krijgen in de precieze werking en mogelijkheden van een tool. DigiTask eist een aanvullende geheimhoudingsverklaring boven op de al door de databeschermer wettelijk vastgelegde geheimhouding.

De Beierse databeschermingsautoriteit voegt een extra element toe aan de vaststelling van de CCC dat derden de DigiTask tool kunnen overnemen door gebrekkige beveiliging van de tool. Uit het Beierse onderzoek blijkt namelijk dat de Beierse politie onzorgvuldig is omgegaan met het gebruik van de spyware.

De gehuurde Amerikaanse server die gebruikt is om de data van de computers van de afgeluisterde verdachten te bewaren, was steeds dezelfde server met hetzelfde IP-adres. De databeschermingsautoriteit acht het niet onwaarschijnlijk dat – wanneer de surveillance door de politie is afgebouwd - een derde de server kan overnemen en de surveillance met dezelfde server

en IP-adres kan voorzetten. Door de publiciteit rondom de DigiTask tool en het rapport van de CCC, waarin het IP-adres wordt genoemd, was het voor iedereen mogelijk het IP-adres te bemachtigen en de specifieke server te huren.

Ook de landelijke databeschermingsautoriteit van Duitsland doet onderzoek. Opnieuw werkt DigiTask tegen en krijgt de databeschermingsautoriteit geen toegang tot de broncode van het bedrijf. Naast een separate geheimhoudingsverklaring wil het bedrijf zelfs 1.200 euro in rekening brengen voor iedere dag en elke werknemer die toegang zou krijgen tot de broncode.

De landelijke databeschermingsautoriteit stelt dat het gebruik van de spyware niet in overeenstemming is met Duitse wetgeving ten aanzien van de integriteit van het persoonlijk leven. Volgens de databeschermingsautoriteit is alle communicatie van verdachten afgeluisterd en opgenomen, waaronder bijvoorbeeld ook momenten van telefoonseks.

Ook is onduidelijk hoe de spyware precies functioneert door gebrek aan documentatie en inzicht in de broncode, functioneert het afluisteren soms niet terwijl de spyware niet is verwijderd van de gegevensdragers, en is het soms niet mogelijk de programmatuur na de afluister operatie te verwijderen. Daarnaast vraagt de landelijke databeschermingsautoriteit zich af waarom spyware is gebruikt en geen contact is opgenomen met de producent van Skype om te assisteren bij de afluisteroperatie.

Hoe vaak wordt spyware ingezet?

De onderzoeken van de CCC en de databeschermingsautoriteiten leiden tot debat in Duitsland over het gebruik van de spyware van DigiTask. En verontwaardiging vanwege de schending van privacywetgeving en de onbetrouwbaarheid van door middel van de inzet van spyware verkregen bewijs. Desalniettemin lijkt het erop dat de Duitse overheid de spyware van DigiTask blijft gebruiken.

Tot ongeveer 2013 hebben maar liefst negen van de zestien Duitse deelstaten (Brandenburg, Beieren, Baden-Württemberg, Hessen, Nedersaksen, Noordrijn-Westfalen, Rijnland-Palts, Saksen-Anhalt en Sleeswijk-Holstein) de spyware van DigiTask gebruikt. Ook de steden Hamburg en Bremen, de landelijke politie, de opsporingsdienst van de Duitse Douane en onder andere de Bundesnetzagentur (de Duitse netwerkbeheerder voor het elektriciteits-, gas, telecommunicatienetwerk) hebben de spyware gebruikt.

Volgens de Duitse overheid wordt spyware alleen ingezet bij de bestrijding van terrorisme en zware georganiseerde criminaliteit. Andere Europese landen claimen hetzelfde. Bij repressieve regimes die hetzelfde beweren blijkt echter keer op keer dat spyware, van bedrijven als Gamma Group (FinFisher), Hacking Team (RCS Galileo en DaVinci) en NSO Group (Pegasus), wordt ingezet tegen oppositieleden, mensenrechtenactivisten, journalisten en andere tegenstanders van de regimes.

Over de inzet van spyware in democratische landen komt meestal weinig naar buiten. De laatste jaren is echter wel van de inzet van de spyware Pegasus van het Israëlische bedrijf NSO in Spanje, Hongarije en Griekenland duidelijk geworden dat het er ook op lijkt dat oppositieleden, journalisten en mensenrechtenactivisten slachtoffer zijn geworden van spyware. De vraag is dus gerechtvaardigd of in hoeverre spyware alleen wordt gebruikt voor de bestrijding van terrorisme en zware georganiseerde criminaliteit.

Het is echter moeilijk om deze claim te onderzoeken. Overheden publiceren over het algemeen nauwelijks gegevens over de inzet van spyware, zoals het aantal en type zaken waarbij spyware is ingezet, het aantal zaken waarbij de inzet tot een veroordeling heeft geleid, en met welke straf. Ook de Duitse overheid publiceert dergelijke gegevens niet.

Zo verklaart de Duitse regering in 2011 dat er sinds 2009 ongeveer 35 keer per jaar spyware werd ingezet. Het gaat hierbij niet alleen om de spyware van DigiTask, de Duitse overheid gebruikt ook spyware van andere bedrijven. Het is niet duidelijk of dit cijfer betrekking heeft op het aantal opsporingsonderzoeken waarbij spyware is ingezet, of het aantal personen of het aantal gegevensdragers die zijn gehackt.

Vanwege het ontbreken van openbare gegevens valt niet vast te stellen hoe betrouwbaar het genoemde aantal van 35 inzetten per jaar is. Verzamelde gegevens uit de media, rapportages van de databeschermingsautoriteiten en andere bronnen over de inzet van DigiTask en andere spyware in Duitsland duiden erop dat spyware in de periode 2007-2013 in ongeveer honderd gevallen is ingezet.

Alleen al in de deelstaat Beieren gaat het om ongeveer 25 verschillende onderzoeken en in Sleeswijk-Holstein om 5 onderzoeken. In de deelstaten Noordrijn-Westfalen, Hessen, Brandenburg en Neder-Sachsen is spyware in twee onderzoeken ingezet. In Bremen, Hamburg, Rijnland-Palts, Baden-Württemberg en Saksen-Anhalt een keer. Ook is spyware in negentien zaken ingezet door de Duitse douane en heeft de landelijke aangegeven dat in 41 zaken computers te hebben geïnfecteerd met spyware.

Wanneer wordt spyware van DigiTask ingezet?

Het is niet duidelijk of in alle bovengenoemde zaken de tools van DigiTask, of andere spyware, is ingezet. Het is evenmin duidelijk of het in alle gevallen ging om onderzoeken naar terrorisme of zware georganiseerde criminaliteit. Het lijkt er echter op dat spyware slechts in een klein aantal gevallen werd ingezet in zaken waarin sprake was van verdenking van terrorisme.

Zo is in Beieren bekend gemaakt dat de regionale Beierse inlichtingendienst (Landesamt für Verfassungsschutz) tot 2011 drie keer gebruik heeft gemaakt van de DigiTask tool bij het afluisteren van mensen die verdacht werden van het voorbereiden van een bomaanslag. Het is niet duidelijk of de inzet tot veroordelingen heeft geleid.

De landelijke politie (BKA) verklaart tussen 2007 en 2011 in 41 gevallen spyware te hebben gebruikt in onderzoeken naar terreurverdachten. In zeven gevallen keer werd niet alleen passief afgeluisterd, maar werd ook de computer op afstand onderzocht met behulp van spyware van bedrijven als DigiTask, Gamma Group en Era IT Solutions AG.

Het is echter moeilijk om de betrouwbaarheid van deze cijfers te duiden en het is de vraag of in het al deze gevallen daadwerkelijk om verdenking van terrorisme ging. Het Duitse landelijk Openbaar Ministerie, dat belast is met de bestrijding van terrorisme in geheel Duitsland, zegt in deze periode namelijk geen gebruik gemaakt te hebben van spyware.

Over negen opsporingsonderzoeken uit de deelstaten Brandenburg, Neder-Saksen en Beieren tot 2012 waarbij spyware is ingezet is meer informatie openbaar geworden en in de media te vinden. Het geeft een indruk van het type opsporingsonderzoeken waarbij de Duitse politie spyware heeft ingezet. Het gaat vooral om drugshandel en andere vormen van smokkel. Uit de openbare informatie wordt niet altijd duidelijk of het in deze zaken tot een veroordeling is gekomen.

Zo werd in Brandenburg spyware ingezet bij een opsporingsonderzoek naar sigarettensmokkel en bij een onderzoek naar de handel in nagemaakte medicijnen, volgens de autoriteiten een vorm van georganiseerde criminaliteit. Bij een van de onderzoeken beschadigde de spyware van DigiTask de harde schijf van de computer van de verdachte dusdanig dat die kapotging. Het is onduidelijk of dit gevolgen had voor het vervolg van het onderzoek, de uiteindelijke vervolging en de strafmaat.

In Neder-Saksen werd de spyware van DigiTask bij twee drugsonderzoeken ingezet. Volgens de autoriteiten ging het wederom om georganiseerde criminaliteit. Het is onduidelijk of het tot vervolging is gekomen.

De Duitse krant *Süddeutsche Zeitung* zet in 2011 vijf opsporingsonderzoeken in 2008, 2009 en 2010 waarbij de Beierse politie spyware van DigiTask heeft ingezet op een rijtje. De krant stelt dat, hoewel het om ernstige vergrijpen gaat, het allemaal niet heel groots (“Auch nichts wirklich ganz Großes”) en ‘geen zware criminaliteit’.

Een van de onderzoeken betreft de verdachte van handel in farmaceutische producten die samen met zijn advocaat Schladt de spyware op zijn laptop ontdekte. Bij de andere onderzoeken gaat het volgens de krant om vergelijkbare criminaliteit zoals handel in verdovende middelen, dopingproducten, gestolen goederen en oplichting. Een van die onderzoeken betreft een groep van vijftien oplichters die honderden elektrische apparaten

op internet aanboden en niet leverden. In totaal werden er ruim honderdduizend slachtoffers gemaakt en verdiende de bende zeven miljoen euro.

De derde en vierde inzet van DigiTask in Beieren draait om een groep helers die gestolen kleding en parfumerie naar het buitenland smokkelden en daar verkochten. Een van de verdachten werd veroordeeld tot twee jaar gevangenisstraf. De andere verdachten kregen lichtere straffen, zoals taakstraffen en geldboetes.

De vijfde inzet betreft een onderzoek naar handel in dopingproducten. De verdachte werd veroordeeld tot vier en een half jaar gevangenisstraf, maar niet zozeer vanwege de handel in doping, maar vooral voor geweldsdelicten in combinatie met diefstal en oplichting. Onduidelijk is bij welk deel van het opsporingsonderzoek de spyware is ingezet.

Tot slot schrijft de krant dat, los van de vijf bovenstaande onderzoeken, de gegevensdragers van drie cannabis handelaren zijn geïnfecteerd met de spyware van DigiTask. Of het hierbij ging om aparte opsporingsonderzoeken of een geheel onderzoek wordt niet vermeld.

De beschikbare informatie duidt er dus op dat de spyware van DigiTask niet alleen is ingezet bij onderzoeken naar terrorisme en zware georganiseerde criminaliteit, maar zeker ook bij minder zware misdrijven.

In latere jaren heeft de Duitse overheid iets meer cijfers gepubliceerd over de inzet van spyware. Zo maakte het Bundesamt für Justiz cijfers bekend over 2019, die een vergelijkbaar beeld opleveren als de beschikbare gegevens over de periode tot 2013. Volgens deze cijfers werd in 2019 in 35 zaken de inzet van spyware gelast. Het ging in 13 zaken om roof met geweld (Rauberische Erpressung) en 12 keer om drugs gerelateerde onderzoeken. De overheid maakt niet duidelijk in hoeveel zaken het tot veroordeling is gekomen en met welke straf. Terrorisme wordt dus niet genoemd in het overzicht. Wel werd de inzet van spyware twee keer gelast bij verdenking op lidmaatschap van een criminele organisatie, en een keer bij landsverraad.

Hoewel het aan uitgebreid onderzoek naar de inzet van spyware in Duitsland ontbreekt, laten de beperkte gegevens zien dat de nadruk bij de inzet niet op terrorisme en zware georganiseerde criminaliteit ligt, maar op minder zware misdrijven.

DigiTask verdient miljoenen euro

Al vanaf de eerste onthulling over het gebruik van DigiTask door de Duitse overheid in 2008 zijn er in de Duitse media bedragen gepubliceerd die door de overheid aan DigiTask, en andere spyware bedrijven, zijn betaald. Er is geen duidelijk overzicht van alle betalingen aan het bedrijf.

Uit mediaberichtgeving en andere onderzoeken wordt echter duidelijk dat DigiTask tussen 2008 en 2013 miljoenen euro van de Duitse overheid heeft ontvangen. Hierbij moet wel aangetekend worden dat het hierbij niet per se om spyware hoeft te gaan, omdat het bedrijf ook andere surveillance middelen, zoals klassieke afluisterapparatuur, videobewaking en data-analyse software, produceert.

De opsporingsdienst van de Duitse douane is een van de grote afnemers van DigiTask. In maart 2008 betaalt het resp. 511.112 en 208.750 euro voor de evaluatie van spyware en hardware en software licenties. Het gaat waarschijnlijk om DigiTask, aangezien later bekend is geworden dat de douane de tools van DigiTask heeft gebruikt. In 2009 ontvangt DigiTask 2.075.256 miljoen euro van de douane voor de levering van haar eigen tool. In oktober 2009 ontvangt het bedrijf 693.672 euro voor het verder in bedrijf houden van de tool, en in 2011 bijna 3,5 miljoen euro.

De Bundeskrimalamt BKA betaalt DigiTask in 2011 200.000 euro. In 2012 moet het bedrijf 423.000 euro delen met Gamma Group en het Zwitserse Era IT Solutions. In 2013 betaalt het Bundesnetzagentur 660.987 aan DigiTask. Hoewel het hierbij om spyware zou kunnen gaan (het Bundesnetzagentur heeft dit namelijk niet ontkend) zou het ook om bewakingsapparatuur van DigiTask kunnen gaan (“TKÜ-TMC, Funk- und Fernsprechüberwachungssystem”).

Deelstaten hebben een flink budget aan de spyware tools van DigiTask besteed. Ook van deze betalingen bestaat geen volledig overzicht, omdat veel deelstaten geen of onvolledige gegevens openbaar hebben gemaakt. Er zijn echter wel indicaties. Zo lijkt de deelstaat Beieren een voorname afnemer te zijn van DigiTask.

In 2006 betaalt de Beierse politie 409.035 euro aan het bedrijf, in 2008 247.773 euro en 614.984 euro. De omschrijvingen bij de betalingen suggereren dat de deelstaat Beieren heeft meebetaald aan de ontwikkelkosten van de spyware. De betaling in november 2008 staat vermeld dat deze is bedoeld voor de "Erweiterung des TKÜ-Systems um ein Archivsystem", de uitbreiding van de spyware tool met een archiveringssysteem.

In totaal betaalt de deelstaat Beieren tot 2013 dertien miljoen euro aan DigiTask. Het is niet bekend of dit bedrag alleen betrekking heeft op de aankoop van spyware, of ook voor andere producten zoals bewakingsapparatuur.

Drie andere deelstaten steken ook miljoenen de aankoop van spyware van DigiTask en andere bedrijven. Niet alleen DigiTask profiteert van die miljoen. Zo betaalt de deelstaat Hessen in 2010 5,3 miljoen euro voor spyware van het bedrijf Syborg onderdeel van het Amerikaanse Verint Systems Inc., nu Cognyte Software Ltd.

Rijnland-Palts betaalde 2,5 miljoen euro ("Lieferung eines TKÜ-Systems") aan een onbekende leverancier. Baden-Württemberg betaalde 1,2 miljoen euro (1.218.225,35) aan de spyware van DigiTask ("TKÜ-System, Lieferung einer TKÜ-Anwendung und Dienstleistung zur Erstellung eines kompletten TKÜ-Systems für die Polizei des Landes Baden-Württemberg").

Andere deelstaten lijken minder aan DigiTask te hebben betaald. In 2012 huurt Noordrijn-Westfalen DigiTask in voor 19.000 euro voor spyware. Een jaar eerder betaalde de deelstaat voor het gebruik van spyware bij twee verdachten 397.714 euro aan concurrent Syborg ("Wartungsvertrag GEMINI ("ist das TKÜ System in NRW").

In 2012 besteedt Noordrijn-Westfalen 400.000 euro aan een nieuwe opdracht voor spyware, maar het is onbekend of DigiTask het enige bedrijf was dat hiervan profiteerde.

Al met al is dus duidelijk dat DigiTask in de loop der jaren miljoenen euro heeft ontvangen van de Duitse overheid. Dit valt ten minste opmerkelijk te noemen, gezien het verleden van corruptie en steekpenningen van het bedrijf.

De miljoenen die de Duitse overheid aan spyware van DigiTask heeft besteed staan in schril contrast met het half miljoen (682.581 euro) dat is uitgetrokken voor de ontwikkeling van een niet-commerciële spyware tool, ontwikkeld door de overheid. Uiteindelijk is die spyware van de overheid nooit operationeel geworden.

DigiTask ook in Nederland gebruikt

DigiTask is in 2018 overgenomen door Rohde & Schwarz. Dit bedrijf uit München maakt elektronica voor test- en meetapparatuur, de ruimtevaart, defensie, mediabedrijven en cybersecurity. In de loop der jaren heeft Rohde & Schwarz ook diverse andere bedrijven overgenomen zoals het in radio monitoring gespecialiseerde Franse Arpège SAS in 2007, het Duitse Ipoque GmbH in 2011 en Sirrix AG in 2015.

De Duitse overheid is de spyware van DigiTask tot waarschijnlijk tot 2014 blijven gebruiken. Ook andere landen waaronder Zwitserland, België en Nederland hebben de tools van het Duitse bedrijf aangeschaft.

Toenmalig Minister van Veiligheid en Justitie Opstelten verklaarde in 2011 dat de Nederlandse politie de spyware van DigiTask heeft aangekocht, nadat dit eerder door het Duitse bedrijf zelf naar buiten was gebracht. Het lijkt erop dat de Nederlandse politie de spyware in ieder geval tot 2014 is blijven gebruiken. De Nederlandse overheid heeft tot nu toe geen openheid van zaken gegeven over de inzet van DigiTask. Woo-verzoeken van Buro Jansen & Janssen blijven deels onbeantwoord, openbaar gemaakte documenten zijn grotendeels onleesbaar gemaakt.