Mag de politie malware van computers verwijderen zonder medeweten van de burger?

De Eerste Kamer moet nog officieel instemmen met het wetsvoorstel computercriminaliteit III, maar op grote veranderingen zullen er waarschijnlijk niet optreden. De meeste aandacht in de discussie over het ontwerpwetsvoorstel computercriminaliteit III is gegaan naar het zogenoemde decryptiebevel, waarin was vervat dat een verdachte kon worden bevolen toegang te verschaffen tot een geautomatiseerd werk (bijvoorbeeld een computer) of delen daarvan, tot een gegevensdrager of tot versleutelde gegevens. Na stevige kritiek van experts heeft de regering besloten dit onderdeel van het voorstel te laten vallen. Toch bevat het wetsvoorstel nog de nodige controversiële bepalingen. Een daarvan is de bevoegdheid van opsporingsambtenaren om zich toegang te verschaffen tot de computer of het device van een verdachte om onderzoek te kunnen doen en bewijs te verzamelen. Ook kunnen gegevens worden gekopieerd en aanpassingen aan de computer worden gedaan, bijvoorbeeld door het verwijderen van malware van de computer van een burger. Deze bevoegdheid zou met name nodig zijn in de strijd tegen botnets.

Het wetsvoorstel kent een nogal brede bevoegdheid toe aan opsporingsambtenaren; verschillende pogingen om meer wettelijke waarborgen neer te leggen en de bevoegdheid verder in te kaderen zijn verworpen. De bevoegdheid ziet blijkens lid 1 van artikel 126nba Sv van het wetsvoorstel op vijf specifieke doelen: (1) het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker; (2) het overnemen van gegevens, zoals bij het vastleggen van afbeeldingen van kinderpornografie of van inloggegevens van besloten groepen of wachtwoorden waarmee de versleuteling van gegevens ongedaan kan worden gemaakt; (3) het ontoegankelijk maken van gegevens, waaronder wordt verstaan het treffen van maatregelen om te voorkomen dat de beheerder van een geautomatiseerd werk of derden verder van de gegevens kennisnemen of gebruikmaken en om te voorkomen dat schadelijke gegevens verder worden verspreid; (4) het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie; en (5) stelselmatige observatie.

Een vrij brede bevoegdheid, waar evenwel een aantal waarborgen op van toepassing is. Zo vereist lid 1 dat er sprake is van ‘een ernstige inbreuk op de rechtsorde’, moet er sprake zijn van een dringend onderzoeksbelang en is de autorisatie van een officier van justitie vereist. Als aan deze voorwaarden is voldaan kan er met behulp van een ‘technisch hulpmiddel’ onderzoek worden gedaan, waarbij het bevel schriftelijk moet worden gegeven en gezien lid 2 ten minste moet bevatten: het misdrijf en een zo nauwkeurig mogelijke aanduiding van de verdachte, de feiten of omstandigheden waaruit blijkt dat de voorwaarden voor de toepassing van deze bevoegdheid zijn vervuld, een aanduiding van de aard en functionaliteit van het technische hulpmiddel dat wordt gebruikt en het doel met het oog waarop het bevel wordt gegeven. Een bevel mag slechts voor vier weken worden gegeven en moet steeds weer worden verlengd (lid 3) en mag slechts worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris (lid 4).

Een aantal commentatoren vindt deze nieuwe bevoegdheid te ruim en heeft gepleit voor de introductie van een nieuw grondrecht dat bescherming biedt tegen deze bevoegdheid. Daarbij wordt met name gewezen op een zaak voor het Bundesverfassungsgericht, waarin het Hof het op afstand uitlezen van harde schijven door de politie en veiligheidsdiensten aan banden legde. Het Hof leidde in deze zaak een nieuw grondrecht uit het algemene persoonlijkheidsrecht af, namelijk de bescherming van de vertrouwelijkheid en integriteit van informatie-technische systemen. Hierbij wordt de computer, tablet en smart phone beschermd

tegen inmenging van derden, zoals de politie, en wordt de daarop opgeslagen gegevens ook beveiligd tegen verandering en compromitterende handelingen.

Een aantal burgerrechtenorganisaties, wetenschappers en parlementariërs heeft zich positief uitgelaten over de mogelijkheid een dergelijk grondrecht ook in de Nederlandse grondwet op te nemen. Het zou een gat opvullen in de huidige bescherming van digitale rechten in Nederland. Toch is hier een aantal vraagtekens bij te plaatsen. Naast de vraag wat onder de definitie van een nieuw te introduceren grondrecht zou vallen is ook de vraag tegen welke inzet van politiebevoegdheden een dergelijk grondrecht bescherming zou kunnen bieden. Het doorzoeken van een computer zou in deze zin gelijk kunnen zijn aan het doorzoeken van een fysieke plaats zoals bijvoorbeeld een woning. In de literatuur en tijdens de parlementaire discussie wordt met name de bevoegdheid om aanpassingen te doen aan de computers van burgers als inbreukmakend gezien. Daarbij moet evenwel worden bedacht dat als deze bevoegdheid door de politie wordt ingezet in de strijd tegen botnets en andere malware, de integriteit van de computer van de burger reeds is gecompromitteerd. In deze zin helpt de politie dus juist de integriteit van de computer te herstellen.

Zowel bij de introductie van de nieuwe politiebevoegdheden als bij de introductie van een nieuw digitaal grondrecht vallen dus de nodige vraagtekens te plaatsen. Dr. Bart van der Sloot, senior researcher aan het Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, heeft in een recent artikel de voor- en nadelen op een rijtje gezet. Lees het volledige artikel hier:
https://www.bjutijdschriften.nl/tijdschrift/TBSH/2017/4/TBSenH_2295-6700_2017_003_004_003