COMMISSION DE L'INTÉRIEUR, DES AFFAIRES GÉNÉRALES ET DE LA FONCTION PUBLIQUE

du

MARDI 4 JUIN 2013

Après-midi

_____

COMMISSIE VOOR DE BINNENLANDSE ZAKEN, DE ALGEMENE ZAKEN EN HET OPENBAAR AMBT

van

DINSDAG 4 JUNI 2013

Namiddag

_____

De vergadering wordt geopend om 14.27 uur en voorgezeten door de heer Siegfried Bracke.
La séance est ouverte à 14.27 heures et présidée par M. Siegfried Bracke.

01 Vraag van de heer Peter Dedecker aan de vice-eersteminister en minister van Economie, Consumenten en Noordzee over"de mogelijke inzet van de 'Big Belgian Firewall' in de strijd tegen PC Bank phishing" (nr. 17714)
01 Question de M. Peter Dedecker au vice-premier ministre et ministre de l'Économie, des Consommateurs et de la Mer du Nord sur "le recours éventuel au 'Big Belgian Firewall' pour lutter contre le phénomène du hameçonnage dans le cadre du PC Banking" (n° 17714)

01.01 **Peter Dedecker** (N-VA): Mijnheer de staatssecretaris, ondertussen heeft het verhaal al redelijk wat *exposure* en reacties gekregen. De Big Belgian Firewall is zo'n beetje een koosnaampje voor iets wat eigenlijk, voor alle duidelijkheid, geen firewall is. Het is enkel een systeem waarmee de grote internetproviders een aantal domeinnamen blokkeren. Als iemand dan naar een van die websites wil surfen, krijgt hij een stoppagina te zien van de FCCU. Men kan dat gemakkelijk omzeilen; dat is geen enkel probleem. De eerste drempel is echter dat men op die pagina terechtkomt.

Destijds werd dat systeem ingevoerd om kinderporno te blokkeren. Ironisch genoeg was de eerste geblokkeerde website stopkinderporno.com. Dat is wel vreemd. Ondertussen zijn er een aantal andere websites aan toegevoegd, onder meer websites van niet-geregistreerde gokdiensten, The Pirate Bay en consorten. Ik heb al gezegd dat het systeem heel gemakkelijk te omzeilen is.

Alleszins moet men zeer voorzichtig zijn met die mogelijkheid, want de stap naar censuur is snel gezet. Denk maar aan The Big Chinese Firewall, wat effectief een firewall is en die men echt niet kan omzeilen. De techniek is echter heel gemakkelijk te omzeilen: voor de liefhebbers, stel gewoon 8888 in als DNS-server en men kan zonder belemmering van de Belgische overheid naar alles surfen wat men wil. Het effect van de DNS-filter is dus zeer beperkt voor wie een beetje ervaring heeft met het internet.

Zo'n minisysteem zou echter wel kunnen helpen in de strijd tegen de massale pc-bankingfraude, waarbij achteloze gebruikers via phishingmails die zogezegd van hun bank afkomstig zijn, wordt gevraagd in te loggen op de *pc banking service*. Zij dienen daarvoor een of andere activatie te bevestigen en belanden zo, zonder dat zij het zelf weten, op een namaakwebsite, waarlangs zij redelijk wat centen overschrijven naar de fraudeur. Dat is een massale plaag voor de Belgische banken. U hebt wellicht ook al massaal veel mails in uw mailbox gekregen zogezegd van de vier Belgische grootbanken, ING, KBC, Belfius en BNP Paribas Fortis. Uit onderzoek blijkt zelfs dat er het voorbije kwartaal een immense toename is geweest: meer dan 2 miljoen euro werd op die manier buitgemaakt. Dat is toch niet weinig.

Is het niet mogelijk om snel dergelijke valse domeinnamen te blokkeren? Het is geen censuur, want men kan dat steeds heel gemakkelijk omzeilen. Het zal ten minste een drempel opwerpen voor wie weinig ervaring heeft met internet en consorten. Die personen zijn trouwens toevallig ook de eerste slachtoffers van dergelijke systemen. Uiteraard is het belangrijk om niet te vervallen in censuur en om de operatoren te beschermen tegen schadeclaims als ten onrechte zo'n site wordt geblokkeerd. Ook transparantie is van het grootste belang. Het is zelfs een noodzaak dat men laat weten welke domeinen op die manier geblokkeerd worden.

Een andere reden is omdat men op die manier kan vermijden dat gebruikers de blokkering omzeilen, bijvoorbeeld om illegale *content* te downloaden, waardoor ze niet langer beschermd zijn.

Daarom heb ik vijf vragen aan u.

Ten eerste, in hoeverre acht u de inzet van het DNS-filtersysteem mogelijk in de strijd tegen pc-bankingfraude via phishing? Hoe zou een dergelijke procedure er voor u kunnen uitzien? Er moet zeer kort op de bal kunnen worden gespeeld, zonder dat men domeinen onterecht blokkeert en tegelijk moet men een onterechte blokkering snel kunnen herzien. Is daarvoor een dienst bevoegd op Belgisch niveau? Ik denk bijvoorbeeld aan FCCU. Is er een dienst die dergelijke meldingen snel zou kunnen beoordelen, die desgevallend kan overgaan tot blokkering en die liefst ook proactief te werk gaat met de Belgische banken?

Ten tweede, is er een mogelijkheid tot bescherming van providers, die vandaag ook reeds de filtertechniek toepassen, maar die misschien vatbaar kunnen zijn voor schadeclaims van derden bij onterechte blokkering?

Ten derde, hoe transparant is het DNS-filtersysteem vandaag? Hoeveel domeinnamen worden vandaag op die manier geblokkeerd? Kan die lijst met domeinnamen niet beter publiek gemaakt worden, net om te vermijden dat het om censuur gaat?

Ten vierde, hebt u enig zicht op het omzeilen van de blokkeringen vandaag? Zoals ik al zei, kan men die eenvoudig omzeilen.

Ten vijfde, welke initiatieven hebt u, en bij uitbreiding de regering, reeds genomen en welke zult u nemen in de strijd tegen phishing, meer bepaald pc-banking phishing bij onze vier Belgische grootbanken?

01.02 Staatssecretaris **Hendrik Bogaert**: Beste collega Dedecker, de Big Belgian firewall is niet de meest efficiënte optie in de strijd tegen phishing, aangezien het blokkeren van domeinnamen alleen kan gebeuren via een juridische beslissing en dus *a posteriori*. De beste methode om phishing te bestrijden, is een informatiecampagne bij de bevolking.

Op 21 mei 2013 lanceerde CERT de website www.safeonweb.be, precies met de bedoeling om het ruime publiek te informeren en te alarmeren op het vlak van informaticabeveiliging. Een campagne die specifiek op phishing gericht is, zou tot stand moeten komen in samenwerking met de betrokken bedrijven, in dit geval met de bankinstellingen.

Persoonlijk stoor ik mij ook aan de talloze mails. Ik meen dat de bankinstellingen in dezen een proactievere rol zouden kunnen spelen en desnoods juridische beslissingen aanvragen of ergens afdwingen. Phishing is geen reclame voor bankieren via internet. Ook het vertrouwen in het algemeen vermindert daardoor. Samenwerking is nodig en ik kan daarbij de betrokkenen alleen oproepen om daarin een proactievere rol te spelen.

Wat uw tweede vraag betreft, in de mate dat de blokkering het resultaat is van een opgelegde juridische beslissing, kunnen de ISP's, de internet service providers, zich op die verplichting beroepen.

Wat uw derde en vierde vraag betreft, noch Fedict noch CERT beheert die lijst. Zij hebben geen zicht op de draagwijdte van de blokkering. U hebt een punt: het systeem is op dit ogenblik weinig transparant. Wij zouden het wat transparanter moeten kunnen maken.

Het belangrijkste is dat het op punt stellen van de cyberveiligheidsstrategie onder andere zal toelaten de strijd tegen phishing op een efficiënte manier aan te gaan.

De cyberveiligheidsstrategie wordt gecoördineerd door de premier. Ik heb daarover al verschillende vragen beantwoord, ook in de Senaat, ook al is het wel degelijk een project van de premier.

Ik kan enkel maar nogmaals wijzen op de urgentie inzake cyberveiligheid. Ik heb dat al eens publiekelijk gedaan. Wij krijgen alsmaar meer signalen dat dat dringend is en ik hoop dat daarmee rekening zal worden gehouden in de volgende budgetronde.

Ik herhaal dat het een bevoegdheid van de premier is. Wij proberen met Fedict en CERT te helpen en het publiek bewust te maken van de problematiek, maar puur formeel komt de bevoegdheid ter zake toe aan de Kanselarij.

01.03 **Peter Dedecker** (N-VA): Mijnheer de staatssecretaris, ik dank u voor uw antwoord, ook al zit de bevoegdheid ter zake grotendeels bij de Kanselarij. Ik hoop dat de Kanselarij ooit een initiatief neemt.

U zegt dat de lijst niet transparant is. Dat is inderdaad een pijnpunt. Het is wel erg om vast te stellen dat de techniek ondertussen al meer dan tien jaar wordt gebruikt en er al die tijd niemand aan heeft gedacht daarin een zekere transparantie te voorzien en een en ander te reglementeren.

Ik hoop dat u alsnog het initiatief zult nemen om te zoeken naar meer transparantie in het systeem. Iemand zal het moeten doen, u of de premier.

U zegt dat bepaalde zaken via een gerechtelijk bevel blokkeren vandaag niet de snelste manier is. Een phishingsite blijft meestal maar een paar dagen actief. Op het ogenblik dat het gerecht zich ermee kan moeien, is het te laat.

Vandaar mijn vraag naar een andere procedure, specifiek gericht op het probleem, waarbij een phishingsite binnen een paar uren geblokkeerd moet kunnen zijn.

Er is daarvoor een andere procedure nodig, samen met de banken. Het heeft geen zin de banken te vragen daarop sneller in te spelen en sneller een blokkering aan te vragen via een gerechtelijk bevel. Zij komen toch grandioos te laat. Ik denk dat het toch wel een stuk sneller zou moeten kunnen via een andere procedure.

De informatiecampagne safeonweb.com is inderdaad, tussen de indiening van mijn vraag en vandaag, gelanceerd. Dat is een heel goede en mooie website. De site is informatief en volgens mij ook begrijpelijk.

Wel is er een klein probleem. Ik vrees ervoor dat het zal verlopen zoals bij zoveel andere goedbedoelde initiatieven in de voorbije jaren, met de beste wil van de wereld en met de beste informatie gelanceerd: het geraakt niet tot bij het doelpubliek. Vroeger hebben er nog massaal dergelijke campagnes plaatsgevonden. Ik vermeld bijvoorbeeld ook dat banken, bij elke mail die zij versturen en bij elk afschrift dat de klant krijgt, de boodschap geven om niet in te gaan op andere websites en om nooit de pincode door te geven via telefoon of mail. Toch lopen veel personen erin en dat is bijzonder bedroevend.

Daarom denk ik dat wij andere maatregelen nodig hebben. Ook technisch zouden enkele zaken volgens mij mogelijk moeten zijn.

Het incident is gesloten.
L'incident est clos.

De **voorzitter**: Vraag nr. 17445 van de heer Thiéry is zonder voorwerp, want de heer Thiéry heeft niets laten weten.

Vraag nr. 17482 van mevrouw Jadin wordt omgezet in een schriftelijke vraag. De toegevoegde vraag nr. 17721 van de heer Deseyn is zonder voorwerp, bij toepassing van het Reglement.

Vraag nr. 17506 van de heer Calvo is zonder voorwerp.

Vraag nr. 17566 van de heer Weyts wordt omgezet in een schriftelijke vraag.

Vraag nr. 17913 van mevrouw Jadin wordt omgezet in een schriftelijke vraag.

Vraag nr. 17989 van mevrouw Gerkens wordt uitgesteld.

Vraag nr. 18124 van mevrouw Jadin wordt omgezet in een schriftelijke vraag.

Vraag nr. 18213 van mevrouw Jadin wordt uitgesteld.

De behandeling van de vragen en interpellaties eindigt om 14.37 uur.
Le développement des questions et interpellations se termine à 14.37 heures.