Question orale de Mme Kattrin Jadin à Annelies Verlinden (Intérieur et Réformes institutionnelles) sur "La cyberattaque contre le SPF Intérieur"

Kattrin Jadin (MR): Monsieur le président, madame la ministre, le SPF Intérieur a été victime d'une cyberattaque, voire d'une probable affaire d'espionnage. Après une analyse approfondie de la part d'experts dans le cadre de la modernisation de son infrastructure informatique, le SPF Intérieur s'est rendu compte qu'un attaquant s'était introduit dans le réseau depuis avril 2019. Le caractère discret de cette introduction laisse présumer un acte d'espionnage. Selon diverses sources, l'attaque a été menée depuis la Chine.

L'affaire est suivie par le parquet fédéral. D'après le CCB, aucune information secrète n'a pu être volée et l'auteur n'avait également pas accès aux données privées de nos concitoyens.

Madame la ministre, que pouvez-vous nous dire sur cette cyberattaque envers vos services? Si des informations secrètes n'ont pas pu être volées, quelles données ont-elles été ciblées et empochées? Quid des auteurs? Lorsqu'ils seront identifiés, quelles conséquences pourront-ils attendre? Et, dans le cas d'une attaque commissionnée par un État, je suppose que cette affaire deviendra bien plus importante. En fonction de votre réponse, je m'enquerrai d'interroger la ministre des Affaires étrangères.

Annelies Verlinden, ministre: Chers collègues, je vous remercie. Il est clair que la visite d'un acteur étatique sur le réseau de l'Intérieur nous pose beaucoup de questions. Comme déjà mentionné en séance plénière, je peux vous communiquer un peu plus de détails sur le dossier sur la base de l'information qui est disponible.

Cette cyberattaque a eu un grand impact sur notre organisation. Après le constat de cette attaque, il fallait, de toute évidence, se défendre. On a donc fait disparaître le malware. On a clôturé les accès directs qui étaient connus de l'attaquant et on a introduit l'*emergency* monitoring. En faisant cela, on peut voir tout ce qu'il se passe sur le réseau pare que cela peut donner des signaux d'autres contaminations ou d'exfiltration de données.

Daarnaast kreeg een projectteam van medewerkers van de FOD Binnenlandse Zaken, van het CCB en externe experts de opdracht om werk te maken van een volledig veilige omgeving, zonder uiteraard de bedrijfsvoering van de FOD in het gedrang te brengen. Alvorens in te gaan op de aanpak voor de toekomst, wil ik eerst nog even de feiten en data op een rijtje zetten.

Op 25 februari van dit jaar zijn er enkele alarmbellen afgegaan bij de ICT-dienst van Binnenlandse Zaken. Er is op 10 maart een HAFNIUM/WebShell-virus op twee *exchange servers* van IBZ ontdekt. Vervolgens is er na verder overleg op 12 maart door CERT.be ontdekt dat er sporen op het netwerk waren die lieten vermoeden dat er meer aan de hand was. Enkele dagen later, op 16 maart, deelde CERT.be mee dat ze sporen van inbraak hadden gevonden op 17 servers en op de *active directory*. De dag erna, op 17 maart, werd ons meegedeeld dat we moesten uitgaan van een ernstige inbraak op het netwerk. Op dat ogenblik was er echter nog geen bewijs van data-exfiltratie gevonden. Twee dagen later, op 19 maart, is aangegeven dat er 20 servers gecompromitteerd waren en op 26 maart is vastgesteld dat er ook bepaalde data geëxfiltreerd waren uit mailboxen van enkele kabinetsleden en van medewerkers van IBZ.

Het CCB heeft na diepgaand onderzoek vastgesteld dat de eerste intrusies merkbaar waren op SharePoint vanaf 30 april 2019. Allerlei tools werden daarbij gedropt op de servers, zoals compressietools en networkscanners. De hackers hebben zich dus vanaf dat ogenblik steeds dieper ingenesteld in het netwerk. Op 18 augustus 2020 werden er sporen teruggevonden van gefaalde exports van data op hun mailservers en werd ook vastgesteld dat er cryptomodules geïnstalleerd waren die detectie bemoeilijken. Op 20 november vorig jaar zijn hackers actief geweest op de servers van de Dienst Vreemdelingenzaken, maar ook op andere systemen van de FOD Binnenlandse Zaken. In totaal kunnen 26 systemen gelinkt worden aan onrechtmatig gebruik door de aanvallers. Ook drie *active directory databases* zijn gecompromitteerd. Ik wil wel opnieuw beklemtonen dat de voor het publiek belangrijke gegevens van het rijksregister, de identiteitskaarten, de verkiezingen en het Passenger Name Record-systeem niet werden gekraakt.

Depuis août 2020, des traces d'accès à 32 boîtes mail, apparemment sélectionnées, ont été trouvées. Les *hackers* se sont emparés d'une quantité de données qui en sont issues. Sur la base des informations disponibles, on peut affirmer qu'elles provenaient de serveurs de messageries électroniques et non de bases de données spécifiques. Cette différence est quand même fondamentale, parce que le parquet fédéral a entre-temps confirmé qu'il n'y a pas eu d'accès à des données à caractère personnel ou à des données classifiées. De telles informations ne se trouvent pas sur le réseau et sont différemment sécurisées.

Nonobstant le fait que les médias ont annoncé que la police était concernée par cette attaque, parce qu'elle dépendrait des services IT de l'Intérieur, je dois vous informer qu'au contraire, l'IT de la police est géré indépendamment de l'Intérieur. Elle ne recourt donc pas au même système. Ainsi, depuis le début de l'année, les boîtes mail individuelles et fonctionnelles de la police intégrée migrent vers le *cloud* Microsoft, qui n'était pas concerné par cette attaque. Aucun problème n'y a été constaté.

Les zones de police locale disposant encore d'un système propre parallèlement à l'officiel ont été immédiatement averties, afin qu'elles prennent les mesures adéquates dans le cas où elles utiliseraient localement un service mail géré en leur sein.

Enfin, je vous informe que le Centre national de crise, l'Autorité de protection des données, la police fédérale, le parquet fédéral, la Sûreté de l'État, le CGRS et le SPF Affaires étrangères ont tous été informés, conformément aux directives définies dans le "Cyberplan d'urgence nationale".

L'enquête judiciaire relative à la cyberattaque est en cours. Un dossier a été ouvert par le parquet fédéral. L'enquête est dirigée par un juge d'instruction bruxellois, après le dépôt d'une plainte avec constitution de partie civile par le SPF Intérieur.

Intussen is ook een plan uitgewerkt om de aanval af te weren. Zoals gezegd, werden in een eerste fase alle dringende maatregelen genomen en in een tweede fase is het risico op verdere intrusie tijdelijk significant verminderd. De gecompromitteerde delen en wachtwoorden werden vervangen en gegevens werden getransfereerd naar een veiligere omgeving. In een derde fase zal het netwerk opnieuw worden opgebouwd en door de implementatie van Proximus *Security as a Service* worden beveiligd.

De verschillende fases bestaan uit diverse deelacties, waarover het projectteam twee keer per week rapporteert. Het gaat om een omvangrijk pakket aan technisch complexe ingrepen.

Chers collègues, si nous nous focalisons sur les possibles auteurs de ces faits, nous voyons que ce dernier est capable de mener une attaque de manière méticuleuse et méthodique, et qu'il a également utilisé des techniques ingénieuses. Il ne s'agit en l'occurrence pas d'une action spectaculaire menée rapidement, mais d'opérations quasi chirurgicales dans lesquelles il se niche très progressivement et de manière quasi invisible dans un réseau.

J'ai demandé à la ministre des Affaires étrangères de lancer la procédure d'attribution de cette cyberactivité malveillante, et le Conseil national de sécurité a approuvé récemment un scénario à cette fin.

En ce qui concerne cette procédure d'attribution, il est vrai que si la Belgique est victime d'une cyberactivité malveillante, une procédure d'attribution diplomatique peut être lancée par un des membres du Conseil national de sécurité si trois conditions sont réunies.

Premièrement, l'implication d'une organisation dite d'importance vitale, ce qui est clairement le cas ici, pour le SPF Intérieur. Deuxièmement, il doit s'agir au moins d'un incident national, voire d'une crise, ce qui est en l'occurrence le cas, étant donné que la phase fédérale a été décrétée. Enfin, le CCB a également indiqué que, compte tenu de la complexité de l'utilisation de techniques avancées et de la persistance de la cyberattaque, on soupçonne l'implication d'une entité gouvernementale, ce qui constitue la troisième condition pour pouvoir entamer une procédure d'attribution.

Sur la base de ces informations, j'ai demandé, en tant que ministre de l'Intérieur, par l'intermédiaire du comité fédéral de coordination, dans le cadre de la phase fédérale, de lancer la procédure d'attribution.

Wat betreft uw andere vragen, over de timing en stappen, de kans op het slagen van de procedure en de gevolgen die eraan verbonden zijn, verwijs ik u naar mijn collega van Buitenlandse Zaken.

Collega's, naar aanleiding van de begrotingscontrole zal eind juni 2021 6,168 miljoen euro beschikbaar worden gesteld, om de complexe cyberaanval het hoofd te bieden, waarvan 5,6 miljoen euro op de IT-werkingskredieten en 500.000 euro op de IT-investeringskredieten.

Voor de urgente vastleggingsdossiers die intussen werden afgerond, werd gebruikgemaakt van de reguliere kredieten van de FOD. Die zullen eind juni gecompenseerd worden door middel van de verkregen kredieten. De concrete aanwending van die middelen situeert zich op vele vlakken, waarvoor ik u desgevraagd graag schriftelijk een overzicht kan bezorgen.

Wij investeren dus meer dan 6 miljoen euro in de veiligheidsmaatregelen, waarmee wij de soevereiniteit van ons land ook verder online beschermen. Cyberspionage komt op steeds grotere schaal voor. De overheid moet zich weerbaarder kunnen opstellen. Dat vraagt om een volgehouden inspanning, waarvoor wij vandaag heel belangrijke stappen zetten.

Kattrin Jadin (MR): Je ne ferai pas de réplique, monsieur le président. C'était très clair et j'ai reçu beaucoup d'informations. Je remercie la ministre.