Hopelijk komt er toch enige kentering en wordt er toch werk gemaakt van een betere bereikbaarheid van de overheid. Ik stel vast dat het op diverse websites toch wel zoeken is om contactgegevens opgespoord te krijgen.

L'incident est clos.
Het incident is gesloten.

10 Question de Daniel Senesael à Alexander De Croo (premier ministre) sur "La vulnérabilité des serveurs Microsoft Exchange" (55016687C)
10 Vraag van Daniel Senesael aan Alexander De Croo (eerste minister) over "De kwetsbaarheid van Microsoft Exchange servers" (55016687C)

10.01 **Daniel Senesael** (PS): Monsieur le président, monsieur le premier ministre, le 14 mars 2021, le Centre pour la Cybersécurité Belgique (CCB) indiquait que "plus de 1 000 serveurs Microsoft Exchange étaient vulnérables", que cette vulnérabilité était activement exploitée par des organisations criminelles et qu'un certain nombre d'organisations et d'entreprises avaient été touchées. Le risque d'un tsunami de cyberattaques contre des organisations vulnérables était alors évoqué.

Le 17 mars 2021, le CCB apportait certaines précisions quant aux causes et à la nature de la vulnérabilité des serveurs de Microsoft Exchange et mentionnait une série d'actions visant à en contrer l'exploitation par des cybercriminels.

Monsieur le ministre, pouvons-nous être informés de l'ampleur des cyberattaques subies par les organisations et entreprises belges jusqu'à présent?

Dans son communiqué, le CCB conseillait aux entreprises et aux organisations qui rencontrent des difficultés avec les étapes indiquées aux organisations et entreprises utilisant Exchange Online - étapes qui, je dois bien l'avouer, semblent assez complexes - de faire appel à un partenaire TIC ou à un expert externe pour effectuer ces actions. Une aide complémentaire provenant du CCB a-t-elle toutefois été offerte aux organisations et entreprises touchées?

La vulnérabilité des serveurs Microsoft Exchange est-elle à ce jour solutionnée?

Enfin, le communiqué du CCB indiquait que certains groupes malveillants installent des *web shells* dans les entreprises, leur permettant l'accès et le contrôle à distance via un serveur en ligne et que, de cette manière, ils peuvent, pour ainsi dire, garder une ligne de communication ouverte avec leurs cibles et lancer des attaques ultérieures. Ceci nous laisse penser qu'un danger pourrait persister pour les organisations et entreprises, même si la vulnérabilité des serveurs était solutionnée. Des solutions destinées à résoudre cet aspect de la problématique sont-elles envisagées?

10.02 **Alexander De Croo**, premier ministre: Monsieur Senesael, Microsoft a découvert le 2 mars une série de vulnérabilités sur le serveur Exchange et annoncé que les hackers les avaient introduites dans de nombreux serveurs informatiques de sociétés, d'organisations et de services publics à travers le monde entier depuis janvier.

Il s'agit d'attaques *zero-day* lors desquelles les pirates exploitent une faille connue dans un logiciel avant que les développeurs en aient connaissance et puissent la corriger.

La période entre le moment où l'on a connaissance de la vulnérabilité et celui de la correction est appelée *zero-day*. Dans ce cas, il s'agissait de la période de janvier à mars de cette année. Ces attaques sont dangereuses car elles sont menées à un moment où aucun protection n'est possible.

Le 3 mars, le CCB a publié un premier avis au sujet des vulnérabilités de Microsoft Exchange. Le 11 mars, le CCB a commencé à envoyer des alertes ciblées à toutes les organisations concernées en Belgique. Au total, le CCB a pu alerter plus de mille entreprises belges utilisant les serveurs Microsoft Exchange.

Près de 95 % d'entre elles ont pris des mesures et effectué les mises à jour nécessaires. À partir des listes de serveurs vulnérables, le CCB a également pu détecter 370 systèmes où une forme d'intrusion avait eu lieu.

Les entités malveillantes ont donc pénétré dans ces systèmes et s'apprêtent à passer à l'action. Pour ce faire, les serveurs criminels installent des *web shells* qui leur donnent un accès et un contrôle à distance via des serveurs en ligne. Ainsi, ils peuvent garder une ligne de communication ouverte pour lancer une attaque par la suite. En plus, les pirates peuvent avoir installé d'autres logiciels malveillants afin de monter une attaque ultérieure, comme par exemple avec un *ransomware*.

Les avis du CCB sont destinés aux responsables IT disposant du bagage nécessaire pour les exploiter. Le CCB aidera toujours mieux les victimes de *ransomware* et de logiciels malveillants et leur fournit divers packs d'informations accessibles qu'elles peuvent utiliser pour détecter et remédier aux problèmes et aux intrusions dans leur système. En réponse aux vulnérabilités de Microsoft Exchange, Microsoft a lancé un outil pour automatiser le processus des clients ayant peu d'expertise informatique.

Dans l'avis et sur les sites internet du CCB et de CERT.be - le service opérationnel du CCB -, il est fait référence à cet outil: le *one click Microsoft Exchange on premises migration tool*. Microsoft met à disposition depuis le 2 mars des mises à jour qui remédient aux vulnérabilités présentes dans les serveurs Microsoft Exchange. Le CCB a fait un rapport détaillé sur ce sujet dans son avis. Les entreprises et organisations utilisant Microsoft Exchange avec une configuration hybride ou un serveur (…) Exchange pour les communications administratives doivent effectuer les actions suivantes: mettre à jour les systèmes; supprimer les *web shells*; vérifier ce qui s'est passé avec les *web shells*; repérer toute activité suspecte.

Microsoft a publié un guide complet de réponse aux incidents, donnant les informations nécessaires. Il y est fait référence dans l'avis et sur les sites web du CCB et de CERT.be, le service opérationnel du CCB.

10.03 **Daniel Senesael** (PS): Monsieur le premier ministre, je vous remercie pour vos réponses.

Vous avez refait l'historique de ces cyberattaques. C'est très intéressant pour reformer le contexte. Merci également pour les actions qui ont été menées, les solutions apportées aux vulnérabilités que vous avez citées. Je pense que c'est vraiment un dossier assez sensible, qu'il conviendra de suivre avec beaucoup de vigilance.

Het incident is gesloten.
L'incident est clos.

11 Samengevoegde vragen van
- Barbara Pas aan Alexander De Croo (eerste minister) over "De maatregelen van het Overlegcomité van 23 april" (55016808C)
- Peter De Roover aan Alexander De Croo (eerste minister) over "Het overlegcomité van 23 april 2021" (55016859C)
- Peter De Roover aan Alexander De Croo (eerste minister) over "De impact van de avondklok op de coronacijfers" (55017155C)
- Peter De Roover aan Alexander De Croo (eerste minister) over "Het Overlegcomité van 11 mei 2021" (55017742C)
11 Questions jointes de
- Barbara Pas à Alexander De Croo (premier ministre) sur "Les mesures prises par le Comité de concertation le 23 avril" (55016808C)
- Peter De Roover à Alexander De Croo (premier ministre) sur "Le Codeco du 23 avril 2021" (55016859C)
- Peter De Roover à Alexander De Croo (premier ministre) sur "L'incidence du couvre-feu sur les chiffres du coronavirus" (55017155C)
- Peter De Roover à Alexander De Croo (premier ministre) sur "Le Comité de concertation du 11 mai 2021" (55017742C)

De **voorzitter**: Mevrouw Pas laat zich verontschuldigen en zal haar vraag nr. 55016808C niet stellen.

11.01 **Peter De Roover** (N-VA): Mijnheer de voorzitter, ik zal mij tot één vraag beperken. Ik heb de twee andere vragen immers al met de eerste minister kunnen bekijken tijdens de plenaire vergadering.

Mijnheer de eerste minister, het spreekt voor zich dat een nachtklok, waarvan wij intussen gelukkig afscheid hebben kunnen nemen, een heel vergaande maatregel is. Wij moeten daar nog even bij stilstaan, omdat het nooit uit te sluiten is dat in de toekomst opnieuw een toevlucht wordt genomen tot dergelijke maatregelen.

Het is erg belangrijk dat wij de impact kennen van een bepaalde maatregel op het fenomeen dat wij willen bestrijden. Het volstaat natuurlijk niet dat wij wat in het rond maatregelen treffen. Wij moeten wel degelijk maat houden en doelmatig en doeltreffend ageren.

Ik heb al een aantal pogingen ondernomen om te weten te komen op welke wetenschappelijke of andere evidencebased basis een beslissing zoals de nachtklok steunt. Tenslotte hebben wij burgers 's nachts thuis opgesloten. Daar komt het immers op neer. Er moeten heel zwaarwegende en goede redenen zijn om dat te doen.

U hebt doorgaans op die vraag geantwoord met veel algemeenheden. In de commissie voor Binnenlandse Zaken van 21 april 2021, waarnaar ik al heb verwezen tijdens de vorige commissiezitting waarop u aanwezig was, antwoordde u het volgende en ik citeer: "Er werd ook gevraagd" – door mij trouwens – "naar het afschaffen van de