**Alexander De Croo (eerste minister) over "Cybersecurity en coronacrisis" (55009190C)**

01.01**Katrien Houtmeyers**(N-VA): Dank u wel, mijnheer de eerste minister om aanwezig te zijn.

In 2019 was er een stijging van 180 % ten opzichte van 2018 wat de aangiftes bij het CERT betreft. Over phishing werden er 1,7miljoen meldingen gemaakt. De economische impact hiervan werd in 2018 al geraamd op 3,5 miljard euro, of meer dan 1 % van het bbp. In 2020, sinds de aanvang van de coronacrisis, wordt er natuurlijk nog meer dan ooit aan telewerk gedaan. We kunnen er enkel van uitgaan dat het aantal aangiften alleen maar groter geworden is en de economische impact alleen maar gestegen is, net nu onze zelfstandigen en kmo's extra kwetsbaar zijn.

Wij hebben absoluut nood aan een meer nationale coördinatie en een sterker waarschuwingssysteem voor veiligheidslekken. Die lekken kunnen immers heel veel schade veroorzaken als ze niet snel opgelost worden.

Het CERT, onze nationale cyberwaakhond, speelt hier natuurlijk een cruciale rol. De organisatie kan bedrijven informeren over hun specifieke kwetsbaarheden. Bedrijven zouden die informatie ook snel moeten krijgen, zeker in het geval van grote veiligheidslekken, precies nu dat onze bedrijven vooral via telewerken functioneren.

Onlangs hoorde ik ook een Europese campagne op de radio met het oog op bewustmaking. Deze campagne werd doorgetrokken naar België, en dat kunnen we enkel toejuichen.

Mijnheer de eerste minister, daarover heb ik een aantal vragen. Van hoeveel bedrijven weet het CERT dat het te kampen heeft met deze kwetsbaarheid? Hoeveel van deze bedrijven heeft het CERT proactief gecontacteerd? Wat wordt daar aan gedaan?

Er wordt ook een onderscheid gemaakt tussen vitale sectoren en andere. Uit deze crisis is gebleken hoe een vitaal bedrijf voor zijn dienstverlening afhankelijk kan zijn van andere niet-vitale bedrijven. Op die manier komt de keten ook in gevaar. Vindt u dit onderscheid dan toereikend? Kunt u mij ook al een overzicht geven van het aantal aangiftes bij het CERT voor de eerste twee kwartalen en indien mogelijk ook voor het derde kwartaal.

Vaak proberen bedrijven een cyberaanval eerst stil te houden uit angst voor reputatieschade. Hoe verhouden de aangiftes zich ten opzichte van de door het CERT vastgestelde aanvallen?

Zijn er nog investeringen en uitbreiding van het personeel van het CERT gebeurd in de laatste maanden? Wat zijn de vooruitzichten omtrent de ondersteuning van onze bedrijven op dit vlak?

Wat de radiocampagne betreft, kunt u een indicatie geven van het netto bereik of het aantal GRP's? Zijn er nog andere communicatiecampagnes gepland?

01.03**Alexander De Croo**, premier ministre: Mevrouw Houtmeyers, monsieur Senesael, je vous remercie pour vos questions, que j'aborderai dans l'ordre dans lequel elles ont été posées.

Mevrouw Houtmeyers, het aantal bedrijven met kwetsbaarheid in België is zeer dynamisch en hangt af van hoe snel die bedrijven zogenaamde patches doorvoeren om de kwetsbaarheden in hun systemen tegen te gaan.

Dagelijks geraken nieuwe kwetsbaarheden bekend en ontvangt het CCB duizenden IP-adressen die kwetsbaar zouden zijn. Identificeren wie eigenaar is van die kwetsbare systemen is zoals in alle EU-landen een zeer grote uitdaging. CERT.be verspreidt geregeld *advisories* met technische informatie over patches voor nieuwe kwetsbaarheden en gerichte waarschuwingen. Dit jaar alleen al waren er 630 van die communicaties, tot nu toe.

Wat uw derde vraag betreft, met organisaties van vitaal belang bedoelt het CCB de publieke en privé-entiteiten die een essentiële dienst verlenen aan de Belgische bevolking en die daarvoor gebruikmaken van netwerk- en informatiesystemen. Deze organisaties die van vitaal belang zijn voor ons land moeten optimaal beschermd worden tegen cyberaanvallen daar incidenten bij deze organisaties een grootschalige nationale impact kunnen hebben voor de maatschappij en voor de nationale veiligheid.

Daarnaast is het belangrijk aan te stippen dat het CCB van elke melding van incident die zij ontvangt beoordeelt of die voldoet aan de criteria om het Nationale Cybernoodplan te activeren, dan wel of het CCB in de mogelijkheid is bijstand te verlenen waar die gevraagd is.

Het CCB publiceert tot slot ook de *supply chain guidelines* die aan aanbieders van essentiële diensten advies verlenen over de controledoelstellingen bij hun toeleveringsbedrijven.

Wat uw vierde en vijfde vragen betreft, dit jaar ontving het CERT tot en met september 5.387 meldingen van burgers, bedrijven en partners. De belangrijkste soorten gerapporteerde incidenten zijn phishingfraude, ransomware, en computervirussen. Deze cijfers geven echter geen volledig beeld. Het reële aantal cyberaanvallen in België is vele malen hoger. Bedrijven en particulieren melden zelden wanneer zij slachtoffer zijn geworden van een cyberincident, en dienen ook niet steeds klacht in bij de politie.

Met uitzondering van enkele aanbieders van essentiële diensten die onder de NIS-wetgeving vallen is er geen meldingsplicht van cyberincidenten. Bovendien zou het kunnen dat het CERT bekender wordt, waardoor meer slachtoffers bij CERT een melding doen. De cijfers maken geen onderscheid tussen particulieren en ondernemingen.

Wat uw zesde vraag betreft, de regering zal voortbouwen op de successen van het Centrum voor Cybersecurity België en heeft de directeur en de adjunct-directrice hiervoor in augustus nog een nieuw mandaat gegeven. Om een gepast antwoord te kunnen bieden aan de sterk toenemende dreiging zal de slagkracht van het CCB de komende jaren eveneens worden versterkt.

Wat uw zevende vraag betreft, het CCB stuurt gerichte notificaties uit als het kennis krijgt dat bedrijven kwetsbaar zijn voor bepaalde cyberrisico's. De acties rond het sensibiliseren en informeren van ondernemingen en rond bijstand in geval van een aanval worden voortgezet en waar mogelijk uitgebreid. Via bewustmaking en de terbeschikkingstelling van technische informatie over de te nemen cyberveiligheidsmaatregelen worden ondernemingen in België aangemoedigd om te investeren in cyberveiligheid. Het sensibiliseren van bedrijven bereikt het CCB via jaarlijkse sensibiliseringscampagnes en via online webinars. Naast bewustmaking informeert het CCB ondernemingen over de te nemen maatregelen om het niveau van cyberveiligheid te verhogen binnen hun bedrijf.

Wat uw achtste vraag betreft, de voorlichtingscampagne wil de Belgische internetgebruiker aanmoedigen om accounts sterk te beveiligen met tweestapsverificatie. Het CCB zet sterk in op een brede mediaverspreiding om de campagne via verschillende kanalen bij de burger te krijgen. De radiocampagne waarvan u melding maakt, is met andere woorden onderdeel van een bredere mediacampagne. In verband met uw vraag over de cijfers met betrekking tot OTH's en GRP's zal u een tabel worden bezorgd.

Wat uw negende vraag betreft, naast de radio worden tijdens de campagne ook andere mediakanalen ingezet. Via advertising op sociale media en Google, televisiespots op de regionale televisie in Vlaanderen, Wallonië en Brussel en advertenties in de krant de *Metro* verspreiden wij de boodschap zo breed mogelijk. Daarnaast helpen ook meer dan 500 partners in publieke, private en academische sectoren de campagneboodschap te verspreiden.

Het CCB ondernam sinds zijn oprichting in 2015 verschillende initiatieven om Belgische burgers te sensibiliseren rond cyberveiligheid. Die initiatieven worden voortgezet. U kunt ook eens de website safeonweb.be bekijken, die beheerd wordt door het CCB en die de Belgische burgers het jaar door op een snelle en correcte manier wil informeren, sensibiliseren en adviseren. Met de campagne in 2017 werd bovendien een e-mailadres gecreëerd om valse berichten naar te versturen. Dat e-mailadres is verdacht@safeonweb.be. Dat initiatief wordt gedurende het hele jaar gepromoot, ook dit jaar.

Monsieur Senesael, les victimes de cybercriminalité peuvent s'adresser à la police locale. Les chiffres concernant le nombre de signalements sont publiés dans les statistiques annuelles sur la criminalité de la police fédérale.

Le CCB ne dispose, dès lors, d'aucun chiffre complémentaire concernant les arrestations et les condamnations de cybercriminels, ni concernant les enquêtes sur les cybercrimes clôturés.

Par ailleurs, ils ne reçoivent pas d'information concernant le profil des suspects. Grâce à l'initiative suspect@safeonweb.be, le CCB reçoit par contre les notifications de *phishing*. Tous les internautes qui reçoivent un message suspect peuvent le transmettre à cette adresse.

Les liens et annexes de ces messages sont, dans ce cas, contrôlés de façon automatisée. Si un lien suspect s'avère positif après être passé au crible du scanner, le CCB fait bloquer les faux URL. Les cybercriminels font ainsi moins de victimes. En 2018, 648 000 messages ont été transmis à cette adresse. En 2019, plus de 1 700 000 messages lui ont été transmis. L'année dernière, quatre cents URL uniques ont été bloqués. Depuis janvier 2020, cette adresse reçoit entre 5 000 et 10 000 faux messages par jour.

Si le CCB constate une augmentation du nombre de signalements, il n'est pas en mesure de conclure si celle-ci est due à une augmentation du nombre d'emails de *phishing* en général, à une meilleure connaissance de l'adresse électronique ou à une combinaison de ces deux facteurs. Le *phishing* demeure le plus grand problème en matière de cybersécurité pour les citoyens en Belgique. À l'avenir, le CCB poursuivra sa lutte contre ce phénomène.

Safeonweb.be dispense des informations et des conseils en matière de cybersécurité. Et à propos des principales menaces qui planent actuellement, il fournit des trucs et astuces afin de surfer en toute sécurité. Il permet aux victimes de cybersécurité de trouver les informations adéquates sur les mesures à prendre.

Le site internet pointdecontact.belgique.be a été élaboré par le Service fédéral Économie pour dénoncer toutes les sortes d'escroquerie, de tromperie, de fraude et de pratiques commerciales illégales. Il s'agit d'un site web où les citoyens et les entreprises peuvent signaler les cas de tromperie, d'arnaque, de fraude ou d'escroquerie. Le site dispense des informations sur les démarches que les victimes doivent entreprendre.

01.04**Katrien Houtmeyers**(N-VA): Mijnheer de eerste minister, bedankt voor uw antwoord.

Uit hoorzittingen over cybersecurity in de commissie voor Economie blijkt dat een erg aanzienlijk deel van de bedrijven hiervoor effectief losgeld betaalt. Ongeacht of er al dan niet losgeld betaald wordt, is de schade voor die bedrijven sowieso heel groot. Wij kunnen dus alleen maar aandringen op meer sensibilisatie, absoluut meer communicatie gericht naar onze bedrijven, kmo's en zelfstandigen. Veel kmo's en zelfstandigen zijn immers elke dag met hun zaken bezig, terwijl cybersecurity voor hen ver van hun bed lijkt of zelfs Chinees is, net zoals corona ver van het bed lijkt of Chinees is, maar in werkelijkheid heel dichtbij is.