**REPONSE DU CONSEIL D'ETAT**
**à l'interpellation Yann Glayre et consorts - Une réaction urgente est-elle nécessaire suite à la fuite de données au ministère de la défense allemand ? (24_INT_44)**

***Rappel de l'intervention parlementaire***

*Hier lundi 4 mars, le ministère de la défense allemand confirmait qu'un enregistrement de 38 minutes d'une séance de visioconférence hautement confidentielle avait été rendu publique par des médias Russes.*

*Les hauts fonctionnaires du gouvernement ont confirmé que la conférence en question s'était tenue sur la plateforme d'hébergement de visioconférence Cisco WebEx, avec des officiers de l'armée de l'air allemande.*

*S'il existe évidemment un doute quant à l'origine de la fuite (celle-ci fait toujours l'objet d'une analyse) cet événement majeur est un signal fort que les solutions 'en nuage' grand public ne peuvent pas être digne de confiance et qu'il vaut mieux, par précaution et souveraineté numérique, utiliser des solutions locales.*

*La DGNSI s'appuie sur la recommandation de la Conférence suisse sur l'informatique (CSI/SIK), qui recommande à ses membres l'utilisation de deux outils : Cisco Webex et Microsoft Teams. Après cette fuite, nul doute qu'une remise en question aura lieu.*

*La télévision ARD parle de "catastrophe" pour les services secrets allemands, et le Chancelier allemand qualifie cette affaire de "très grave pour l'Allemagne". Nous sommes donc au coeur d'une guerre de l'information qui ne fait que commencer.*

*Compte tenu que Cisco WebEx est l'un des moyens de communication majeur du canton, par notamment les systèmes de téléphonie WebEx Calling, j'adresse au Conseil d'Etat les questions suivantes :*

*1) Peut-on encore faire confiance à la plateforme Cisco WebEx pour les activités de télécommunications de l'Etat de Vaud ?*

*2) Des séances du Conseil d'Etat ou de hauts responsables cantonaux sont-elles régulièrement tenues et enregistrées sur Cisco WebEx ?*

*3) Si tel est le cas, est-ce que cette affaire a amené le Conseil d'Etat à revoir les pratiques en vigueur ?*

*4) L'adoption d'une solution suisse 'qualité militaire' pour la téléphonie et la visioconférence pourrait-elle être envisagée ?*

*Je remercie le Conseil d'Etat pour ses réponses et sa promptitude à réagir à cette situation pour le moins inconfortable.*

**Réponse du Conseil d'Etat**

**Préambule**

La cybersécurité est une préoccupation majeure du Conseil d'Etat. Elément clé de sa stratégie numérique et de son programme de législature, elle figure parmi les objectifs principaux du plan directeur cantonal des systèmes d'information, qui guide l'action de la Direction générale du numérique et des systèmes d'information (DGNSI). A ce titre, cette dernière a œuvré à constamment renforcer son système de management de la sécurité de l'information et a obtenu à ce jour deux certifications internationales, ISO 9001 et 27001, attestant de la qualité des mesures mises en place. Au surplus, il est utile de rappeler que le Canton joue un rôle clé dans la sécurité et la veille sur les vulnérabilités pour les institutions publiques vaudoises, notamment pour les communes vaudoises, au travers de la Convention Canton-communes signée en 2023.

Le développement de l'environnement de travail numérique, qui consiste à mettre en place des outils de travail numérique répondant aux besoins des collaboratrices et collaborateurs de l'ACV, suit cette même politique. La solution Webex de l'entreprise Cisco a été déployée en 2020 pendant la pandémie pour permettre à l'Administration cantonale vaudoise (ACV) de continuer ses activités et ses missions, puis pérennisée pour permettre le développement du télétravail et la mobilité des collaboratrices et collaborateurs de l'ACV.
Pour rappel, ce produit logiciel Webex a fait par ailleurs l'objet d'une analyse dédiée de sécurité et de protection des données. Le Conseil d'Etat renvoie à cet égard à l'analyse détaillée présentée dans sa réponse au postulat Jean-François Chapuisat – Pour une solution de visioconférence fiable, conviviale, et sécurisée ! (20_POS_220), qui confirme l'adéquation du produit sur les trois axes de la sécurité, de la convivialité et de la fiabilité. Pour rappel, l'instance utilisée par l'ACV est déployée sur des serveurs européens, et est conforme aux exigences légales vaudoises en matière de protection des données.

*Question 1 : Peut-on encore faire confiance à la plateforme Cisco WebEx pour les activités de télécommunications de l'Etat de Vaud ?*

En préambule, il convient de rappeler que Cisco Webex est un des outils majeurs de collaboration, choisi par la DGNSI, parce qu'il offre un large éventail de fonctionnalités pour les communications et la collaboration en équipe. A l'ACV, les principales fonctionnalités utilisées sont les réunions en ligne, la messagerie instantanée et les appels téléphoniques, y compris vidéo. Lors de son intégration et de sa paramétrisation pour l'ACV, une attention particulière a été portée à la sécurité et la protection des données. Malgré les précautions prises par la DGNSI selon des standards reconnus, tout composant informatique, qu'il soit matériel ou logiciel, peut, au cours de son cycle de vie, être affecté par des vulnérabilités. La DGNSI travaille en permanence à anticiper les effets de ces vulnérabilités et, lorsqu'elles surviennent, à les corriger dans les plus brefs délais.
Concernant l'incident de sécurité rapporté par le Gouvernement allemand et selon les informations publiquement disponibles, la fuite résulterait du fait qu'une personne ait rejoint la séance Webex en question via un appel téléphonique depuis son téléphone et non au travers de l'application mobile Webex, qui garantit des échanges cryptés et sécurisés de bout en bout. Avec toutes les précautions d'interprétation des informations diffusées dans un contexte de conflit international et où la désinformation est une arme largement utilisée par les belligérants, la compromission serait ainsi due à une configuration inadéquate de Webex permettant une connexion via une ligne téléphonique, plutôt qu'à une vulnérabilité intrinsèque.

La veille et les recherches menées par le Centre opérationnel de sécurité de la DGNSI, le SOC, en collaboration avec l'Office fédéral de la cybersécurité (OFCS), n'ont pas permis de détecter une faille qui aurait provoqué cet incident. A ce stade, et selon les experts du domaine, la piste privilégiée pour expliquer l'incident en question est une mauvaise configuration de l'instance de l'armée allemande. Le fournisseur Cisco nous a par ailleurs formellement certifié, suite à notre requête, l'absence d'une faille de sécurité dans le système de cryptage de Webex et de toutes autres failles de sécurité connues à ce jour sur leur système. Il est aussi à noter que, le 5 mars 2024, le ministre de la Défense allemand, Monsieur Boris Pistorius, a publiquement précisé que leurs systèmes de communication n'avaient pas été compromis[1].

Néanmoins, dans un souci d'amélioration continue, la DGNSI a pris les mesures suivantes afin de renforcer la sécurité de l'utilisation de la plateforme Webex :

- Automatisation de l'activation d'un code de déverrouillage sur les appareils mobiles non fournis par la DGNSI qui utilisent Webex ;
- Blocage des accès audios par un numéro d'appel afin d'éviter l'accès aux séances par un canal non crypté.

[1] https ://www.politico.eu/article/german-defense-minister-blames-taurus-call-leak-officer-logging-via-insecure-hotel-line/

Par ailleurs, il est important de rappeler que le Conseil d'Etat veille à régulièrement former les collaboratrices et collaborateurs de l'ACV aux bonnes pratiques de sécurité informatique par l'organisation de campagnes de sensibilisation, et s'assure qu'ils soient rendus attentifs aux règles d'usages propres aux outils mis à disposition. La DGNSI a publié des bonnes pratiques détaillées[1] pour l'utilisation de la vidéoconférence et de l'outil Webex en particulier. Elles sont destinées aux organisateurs de séances d'une part et aux participants d'autre part.

Suite cet incident, et à la lumière des explications reçues par Cisco, des investigations menées par la DGNSI et l'OFCS, des actions de renforcement de la sécurité et des informations mises à disposition du personnel de l'Etat, le Conseil d'Etat constate qu'il n'existe pas à ce jour d'éléments de nature à remettre en question l'usage de la solution Webex au sein de l'ACV. Il reste néanmoins très attentif à l'évolution des cybermenaces et prendra les mesures supplémentaires qu'il jugera nécessaires pour garantir la sécurité des informations de l'ACV.

*Question 2) Des séances du Conseil d'Etat ou de hauts responsables cantonaux sont-elles régulièrement tenues et enregistrées sur Cisco WebEx ?*
*Question 3) Si tel est le cas, est-ce que cette affaire a amené le Conseil d'Etat à revoir les pratiques en vigueur ?*

Le Conseil d'Etat tient ses séances en présentiel. Par le passé, il n'a eu recours à l'outil Webex qu'à quelques reprises seulement durant la période Covid, puis à quelques occasions extrêmement rares et de manière partielle, à savoir durant quelques minutes de séance pour échanger avec un membre momentanément absent. Dans aucun cas la séance n'a été enregistrée. Le Conseil d'Etat reste très attentif au secret de ses débats, tel que prévu dans la loi. Au vu du recours très limité à cet outil, il n'y a pas lieu de revoir sa pratique actuelle.

*Question 4. L'adoption d'une solution suisse 'qualité militaire' pour la téléphonie et la visioconférence pourrait-elle être envisagée ?*

Par rapport à cet incident rapporté par la presse, il convient de rappeler que les mécanismes d'encryption utilisés par Cisco Webex répondent aux bonnes pratiques et standards de sécurité du moment et que la veille menée par les spécialistes sécurité de la DGNSI n'a identifié aucune faille de sécurité connue.

La DGNSI recommande de tenir des séances hautement confidentielles, stratégiques ou en lien avec un évènement exceptionnel en présentiel afin d'éviter des fuites d'information et de mettre en œuvre les bonnes pratiques préconisées lors de la tenue de séances virtuelles.

En conclusion, le Conseil d'Etat considère que le remplacement de la solution Webex ne se justifie pas. Le système de chiffrement de la solution de vidéoconférence ne présente pas de signe de faille de sécurité, et le cas d'espèce résulte certainement d'une mauvaise utilisation de la solution. Le Conseil d'Etat reste toutefois attentif et continuera, avec l'expertise de la DGNSI, d'effectuer une veille sécuritaire sur ce sujet, et à poursuivre la formation des collaboratrices et collaborateurs aux bonnes pratiques de sécurité informatique.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 12 juin 2024.

| La présidente : | Le chancelier : |
| --- | --- |
| *C. Luisier Brodard* | *M. Staffoni* |

[1] https://www.vd.ch/toutes-les-autorites/departements/departement-de-la-culture-des-infrastructures-et-des-ressources-humaines-dcirh/direction-generale-du-numerique-et-des-systemes-dinformation-dgnsi/videoconference-bonnes-pratiques