Organisation mondiale de la Santé

CONSEIL EXÉCUTIF **EB148/30**
Cent quarante-huitième session **11 janvier 2021**
Point 18.1 de l'ordre du jour provisoire

Le point sur la gestion et la technologie de l'information

Rapport du Directeur général

1. Lors de la trente et unième réunion du Comité du programme, du budget et de l'administration du Conseil exécutif en janvier 2020, le Secrétariat a présenté ses initiatives en matière de cybersécurité.[1] En outre, le dernier rapport du vérificateur intérieur des comptes,[2] examiné à la trente-deuxième réunion du Comité, signalait les principaux éléments de la vérification de la feuille de route pour la cybersécurité. Le présent rapport fait suite à la demande adressée par le Comité au Secrétariat afin que celui-ci donne des informations sur la gestion de la cybersécurité.

PROGRÈS AVANT LA PANDÉMIE

2. La cybersécurité est l'un des principaux domaines de la stratégie sur la gestion et la technologie de l'information dans lesquels il s'agit d'obtenir des résultats. Elle vise à protéger les actifs numériques du Secrétariat, à renforcer la sécurité des données et à garantir la possibilité de fournir des services tout en maintenant un niveau de risque acceptable.

3. Plusieurs initiatives ont été entreprises en faveur de la cybersécurité, dont la mise en œuvre d'une formation obligatoire à l'échelle de l'Organisation pour la sensibilisation à la cybersécurité ; des exercices mensuels sur le hameçonnage ; l'organisation d'un événement annuel de sensibilisation à la cybersécurité ; la création d'une archive centrale de journaux système à des fins d'enquête ; la standardisation de la gestion des pare-feu ; le déploiement d'un antivirus à l'échelle mondiale ; la mise en place d'un service de filtrage du trafic Internet ; et le recueil de renseignements sur les menaces afin que des mesures préventives puissent être prises pour éviter la survenue d'incidents prévisibles.

4. Le Secrétariat a également créé une équipe indépendante chargée de la cybersécurité. Il a aussi mis en place un centre intégré d'opérations de sécurité, couvrant l'identification, la prévention et la détection des cyberattaques, ainsi que la protection et les interventions lorsqu'elles se produisent.

[1] Document EB146/40.

[2] Document A73/28.

5. La gouvernance a été renforcée avec la publication de la stratégie de cybersécurité approuvée, de la feuille de route pour la cybersécurité et d'une politique, de règles, de normes et de modes opératoires normalisés à l'échelle mondiale ; la création du Conseil de cybersécurité ; et la révision de la Charte du Comité d'orientation de la technologie de l'information pour répondre à la nécessité d'une responsabilité globale en matière de cybersécurité.

MESURES PRISES FACE AUX ATTAQUES LIÉES À LA COVID-19

6. Depuis que la pandémie de COVID-19 a été déclarée, le Secrétariat a observé une augmentation du nombre de cyberattaques ciblées : *spear phishing* (harponnage), usurpation d'identité, hameçonnage, hameçonnage vocal et attaques contre l'infrastructure et les applications informatiques. Entre mars et mai 2020, plus de 130 000 domaines liés à la COVID-19 ont été enregistrés, dont 70 % étaient faux et ont été utilisés pour de multiples cyberattaques, selon des chercheurs.

7. Les cyberattaques sont toujours plus nombreuses et plus complexes. La solution initialement appliquée pour recueillir des renseignements sur les menaces a été jugée insuffisante. Une nouvelle solution mise en œuvre le 7 mai 2020 a fait apparaître d'autres menaces persistantes avancées. Elle a permis au Secrétariat d'agir plus rapidement pour remédier l'infrastructure, les systèmes et les outils informatiques existants.

8. Toutefois, selon les analyses de tendances effectuées par des entreprises spécialisées dans la cybersécurité, les cyberattaques devraient se poursuivre. Les efforts visant à identifier, prévenir et détecter ces cyberattaques, à s'en prémunir, à intervenir pour y faire face et à s'en relever doivent être continuellement intensifiés. Le Secrétariat a donc accéléré la mise en œuvre du programme de cybersécurité. **Des mesures essentielles ont été prises,** dont celles présentées ci-dessous.

a) **Financement.** Selon le rapport du vérificateur intérieur des comptes d'octobre 2020,[1] les 1,3 million de dollars des États-Unis reçus ne suffisaient pas à mettre en œuvre la feuille de route pour la cybersécurité. Le Comité d'orientation de la technologie de l'information a fourni 4,7 millions de dollars des États-Unis supplémentaires. Le programme dispose donc de 6 millions de dollars des États-Unis au total.

b) **Équipe de cybersécurité.** L'équipe, qui comptait six membres, en compte désormais 11, en poste à Genève ou à Budapest. Une équipe rouge a été mise sur pied pour prendre des mesures énergiques en vue de vérifier la sécurité des systèmes informatiques, notamment de repérer les vulnérabilités du système et d'évaluer les risques.

c) **Création d'un centre d'opérations de sécurité géré et intégré.** Un centre d'opérations de sécurité géré, où les opérations de sécurité sont intégrées à un service de gestion d'informations et des événements liés à la sécurité, a été mis en place en juin 2020. Le centre donne des informations sur tous les incidents de sécurité et permet au Secrétariat de se concentrer sur les événements qui doivent faire l'objet d'une attention particulière. Entre août et novembre 2020, 14,5 milliards d'événements de sécurité ont été recensés. Grâce à la mise en place du centre d'opérations de sécurité, le Secrétariat a pu filtrer, traiter et analyser 243 incidents de sécurité nécessitant une attention particulière et y concentrer ses efforts.

[1] Document A73/28.

d) **Authentification renforcée des utilisateurs.** Le Secrétariat renforce les méthodes d'authentification traditionnelles (telles que l'authentification par le nom d'utilisateur et le mot de passe) en ajoutant des services d'authentification multifactorielle (par exemple à l'aide d'un *soft token*) pour que les utilisateurs prouvent leur identité. L'application intégrale de l'authentification multifactorielle est achevée et couvre tous les services du Secrétariat disponibles sur Internet.

e) **Suivi continu des actifs informatiques de l'Organisation.** Le Secrétariat a mis en œuvre une solution de détection et d'intervention sur les terminaux pour pouvoir suivre en continu les menaces contre les actifs informatiques de l'Organisation et intervenir en utilisant des outils pour détecter et endiguer (si nécessaire) les activités suspectes, et mener des enquêtes. Cette solution offre de la visibilité dans l'environnement de travail et donne les moyens de détecter, de protéger et d'intervenir rapidement. À ce jour, 88 % des ordinateurs et des serveurs de l'Organisation sont couverts et des travaux sont en cours pour parvenir à 100 % d'ici au deuxième trimestre 2021.

f) **Système pour empêcher l'usurpation d'identité avec une adresse de courriel de l'Organisation à destination du public.** En moyenne, 2,3 millions de courriels uniques sont envoyés chaque mois sous le nom de domaine <@who.int>. En avril 2020, environ 80 % de ces courriels correspondaient à une usurpation d'identité. En mai 2020, le Secrétariat a mis en œuvre une solution DMARC (domain-based message authentication, reporting and conformance) afin d'éviter autant que possible les usurpations d'identité et de ne permettre qu'aux sources autorisées d'envoyer des messages au nom de l'Organisation. Depuis, 96 % des courriels sont conformes et les 4 % restants impliquant des usurpations d'identité ont été supprimés et ne sont jamais parvenus dans les boîtes aux lettres des organisations qui ont mis en œuvre des solutions DMARC.

g) **Retrait d'applications anciennes.** Les anciens systèmes développés à l'aide d'une technologie obsolète sont vulnérables en cas d'attaque sophistiquée. Des correctifs de sécurité sont appliqués, mais, dans certains cas, la conception et l'architecture obsolètes du système font que ces correctifs ne sont pas suffisants pour contrer les attaques malveillantes. Le Secrétariat a donc remplacé un grand nombre d'applications qui ne peuvent plus être remédiées ou pour lesquelles il est impossible d'utiliser un correctif.

9. Pour que le programme de cybersécurité soit géré efficacement, la communication et la coordination doivent être constantes. En particulier :

a) en interne, la coordination mondiale passe par le groupe de cybersécurité, qui est composé de l'équipe de cybersécurité et de représentants de toutes les Régions. Ce groupe coordonne les activités de l'OMS liées à la cybersécurité, y compris l'application de procédures, de normes et de solutions en matière de cybersécurité ;

b) un canal de communication directe a été mis en place avec plusieurs équipes informatiques d'intervention d'urgence, des organisations gouvernementales et des entreprises privées afin de recevoir et d'échanger des renseignements sur les menaces afin de prendre des mesures. Des indicateurs de compromission sont communiqués quotidiennement.

10. En outre, les systèmes et applications institutionnels – dont le Système mondial de gestion, le courrier électronique, les sites Web, les plateformes de collaboration et les plateformes de développement – sont constamment surveillés et des correctifs de sécurité sont appliqués sans délai pour réduire ou éliminer les risques liés à la cybersécurité.

PÉRENNISATION DES EFFORTS EN MATIÈRE DE CYBERSÉCURITÉ

11. Les atteintes et les attaques liées à la cybersécurité, lorsqu'elles sont couronnées de succès, sont coûteuses. Les coûts potentiels comprennent l'atteinte à la valeur et à la réputation du Secrétariat ; la perte financière directe (remédiation, temps de travail, frais juridiques, frais de relations publiques et frais de notification) ; l'incidence sur la disponibilité des systèmes ; la perte de données essentielles ; et l'atteinte à l'intégrité des données.

12. Malgré tous les efforts susmentionnés déployés par le Secrétariat, il reste encore des lacunes à combler et des améliorations à apporter dans plusieurs domaines. Les huit nouveaux axes de travail suivants sont essentiels pour protéger le Secrétariat contre les acteurs qui représentent une menace persistante avancée et ils sont inclus dans le programme de cybersécurité.

a) **Amélioration de la protection du courriel et sécurité des liens et des pièces jointes.** Plus de 90 % des cyberattaques commencent par un hameçonnage par courriel à l'aide de liens et de pièces jointes. Les fonctionnalités intégrées de sécurité des courriels offriront une protection grâce à une recherche automatique améliorée de contenu malveillant dans les pièces jointes, et les clics dans les courriels seront vérifiés.

b) **Accès plus sûr à Internet**. L'utilisation d'un proxy sur le cloud à l'échelle mondiale assurera la protection des terminaux accédant à Internet, tant à l'intérieur qu'à l'extérieur des bureaux de l'Organisation. Ce dispositif permet de contrôler l'accès à Internet à partir des terminaux grâce à la vérification des sites Web, au filtrage et à la protection contre les logiciels malveillants.

c) **Scanner de vulnérabilité des applications.** Ce dispositif permet d'évaluer de manière plus cohérente la sécurité des applications mobiles et sur le Web pendant le développement, les tests et l'exploitation. Il s'agit de repérer les vulnérabilités du système, du réseau et des applications.

d) ***Web application firewall*.** Il s'agit d'une nouvelle génération de protection et d'accès pour les applications Web. Un *web application firewall*, qui agit à la fois comme bouclier et comme passerelle, est placé entre les applications Web et Internet et protège les applications des attaques. Les accès externes sont contrôlés, filtrés et surveillés.

e) **Contrôle des vulnérabilités.** Ce dispositif crée un système de vérification et de notification automatiques en ligne qui sera intégré aux processus de gestion des incidents, des changements et des correctifs. Il facilitera la remédiation des vulnérabilités liées aux systèmes et applications sans correctifs.

f) **Gestion des accès privilégiés.** Ceci permet non seulement à l'Organisation de connaître les menaces potentielles posées par divers types d'accès privilégié, mais aussi, moyennant l'utilisation d'outils appropriés, d'éviter l'utilisation abusive de comptes à privilèges élevés (tels que ceux des administrateurs système).

g) **Gestion de la séparation des tâches.** Ceci garantit une division claire des tâches et des rôles concernant l'accès aux systèmes. En aucun cas une personne ne devrait être en mesure d'effectuer et d'approuver des opérations afin de commettre un cyberdélit (vol ou fraude à des fins d'enrichissement personnel).

h) **Technologie de la tromperie.** Il s'agit de créer des pièges ou des leurres pour faire croire aux acteurs à l'origine de menaces qu'ils ont réussi à pénétrer au sein l'Organisation (par exemple pour voler des informations d'identification ou des secrets). Ainsi, le Secrétariat sera mieux à même de détecter le comportement des intrus et d'utiliser ces informations pour renforcer la sécurité de ses systèmes.

13. Il est essentiel de maintenir l'élan. L'inclusion de ces axes de travail dans les démarches entreprises par le Secrétariat en matière de cybersécurité renforcera encore les modalités d'identification, de détection, de prévention, de protection et d'intervention conduisant à la mise en œuvre de la feuille de route pour la cybersécurité.

PÉRENNITÉ DU FINANCEMENT

14. Dans sa décision WHA70(16) (2017), l'Assemblée mondiale de la Santé a autorisé le Directeur général à allouer, à la fin de chaque exercice, au moins 15 millions de dollars des États-Unis, selon les disponibilités, aux besoins d'investissement dans les technologies de l'information dans le cadre du Fonds pour les infrastructures.[1] Le programme de cybersécurité actuel est financé par le Fonds pour les infrastructures.

15. Le Secrétariat considère la cybersécurité comme une priorité absolue. Il est important de préserver tous les acquis obtenus à ce jour et de poursuivre le travail accompli pour protéger l'Organisation. De premières estimations des coûts ont été établies afin d'achever le programme de cybersécurité. Toutefois, le maintien des opérations de cybersécurité après l'achèvement du programme nécessitera également des investissements importants dans les années à venir.

16. Le Comité consultatif indépendant d'experts de la surveillance a recommandé qu'un examen global des dépenses consacrées à l'informatique par l'Organisation soit entrepris dans le cadre du cycle global de planification.[2] Cet examen devrait tenir compte à la fois des coûts de fonctionnement du Secrétariat et de toutes les initiatives de changement dans le domaine de l'informatique, y compris de la cybersécurité. Le Secrétariat procède à cet examen dans le cadre de l'établissement du projet de budget programme 2022-2023.

17. Le Secrétariat communiquera aux États Membres, par l'intermédiaire du Comité du programme, du budget et de l'administration à sa trente-quatrième réunion, le ratio des initiatives (le nombre d'opérations par rapport aux changements) et un examen global actualisé des dépenses futures qui seront consacrées à l'informatique.

MESURES À PRENDRE PAR LE CONSEIL EXÉCUTIF

18. Le Conseil est invité à prendre note du présent rapport

= = =

[1] Voir le document WHA70/2017/REC/1.

[2] Voir le document EBPBAC30/2.