PRIMATURE

SECRETARIAT GENERAL

AGENCE NATIONALE DE SECURITE
DES SYSTEMES D'INFORMATION

Burkina Faso
Unité-Progrès-Justice

N°2020_____/PM/SG/ANSSI/DG

*Ouagadougou, le* 14 AVR 2020

# COMMUNIQUE

Face à la crise pandémique du coronavirus (COVID-19), l'État Burkinabè à travers le département en charge de la santé a mis en place des mesures devant permettre d'endiguer ce fléau. Ces mesures prises ne sont pas sans répercussion sur le mode de fonctionnement des administrations et des entreprises. Pour assurer la continuité du service, l'utilisation des méthodes de télétravail a été fortement encouragée. Toutefois, mal préparé, le saut vers le télétravail ainsi que les nouvelles pratiques exposent l'administration, les entreprises et leurs systèmes d'information à des risques d'attaques informatiques.

L'ANSSI souligne le caractère bénéfique de ces outils de travail, mais attire l'attention des administrations et des entreprises sur leur utilisation qui n'est pas sans risques (accès frauduleux aux échanges, vol de données, chantage...).

Par ailleurs, elle invite les structures désirant mettre en œuvre les outils de télétravail, à évaluer les risques y afférents en tenant notamment compte de toutes les caractéristiques techniques de ces outils.

Aussi, recommande-t-elle entre autres :

- l'implémentation des outils de télétravail au niveau national et hébergés sur les serveurs nationaux ;
- qu'une sécurisation du DNS (Domain Name System )puisse précéder la mise en œuvre des outils de télétravail pour permettre de lutter efficacement contre les malveillants ;

- l'implémentation de l'authentification à double facteurs pour combattre les attaques par force brutes, par dictionnaire, etc. ;
- l'utilisation de gestionnaire centralisé des mots de passe pour non seulement garantir la complexité mais aussi la mise à jour régulière ;
- la mise en place des canaux sécurisés par l'implémentation des VPN (réseaux virtuels privés) afin de rendre chiffrées les communications ;
- les sauvegardes systématiques et régulières de l'information traitée pour faire face aux attaques de type ransomwares ;
- l'application systématique des derniers correctifs de sécurité aux équipements et logiciels utilisés (VPN, solution de bureau distant, messagerie, vidéoconférence, etc.).

L'être humain, étant au début et à la fin de la chaine de la sécurité des systèmes d'information, l'ANSSI exhorte fortement les utilisateurs à adopter un comportement cyberprudent pour lutter efficacement contre les attaques malveillantes.

Pour tout besoin d'accompagnement, les structures désireuses de mettre en œuvre les outils de télétravail sont invitées à s'approcher de l'ANSSI ou de toute autre entreprise spécialisée dans la sécurité des systèmes d'information.

**Le Directeur Général**

Agence Nationale de Sécurité des Systèmes d'Information * ANSSI * Directeur Général

**Michaël Guibougna Lawakiléa FOLANÉ**