ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

NOTE D'INFORMATION N° 24100304/20

OBJET : RECOMMANDATIONS DE CYBERSECURITE LIEES AU TELETRAVAIL

La crise sanitaire mondiale du COVID-19 a nécessité la mise en place de mesures de confinement et de limitation des déplacements aux seuls motifs indispensables. Face à cette situation exceptionnelle et inédite, les administrations, entreprises ou collectivités, désignés ci-après entités, qui en avaient la possibilité ont dû mettre en place le télétravail pour préserver les activités essentielles que ce mode de fonctionnement peut permettre.

Cependant, une mise en œuvre non-maîtrisée du télétravail peut augmenter les risques de sécurité pour les entités qui y recourent. Elle peut même mettre en danger leur activité face à une cybercriminalité qui redouble d'efforts au cours des dernières années.

Dans la suite de la note d'information diffusée en date du 20 mars 2020 auprès des Responsables de la Sécurité des Systèmes d'Information (RSSI), la présente note a été élaborée par la Direction Générale de la Sécurité des Systèmes d'Information pour décrire les mesures de sécurité à prendre afin de mieux maîtriser les risques liés au télétravail.

A. PRINCIPAUX RISQUES ET CYBERMENACES LIES AU TELETRAVAIL

Dans ce contexte inédit caractérisé par le recours au télétravail, les entités sont plus exposées à des risques et attaques informatiques. Ces attaques ont pour principaux objectifs :

- **Vol ou altération de données :** Les attaquants tirent profit des mesures de sécurité réduites en dehors des locaux de l'entité pour accéder aux données présentes sur les postes de travail. En effet, à domicile, les postes de travail sont directement exposés au réseau Internet sans protection appropriée (absence de filtrage des flux, présence d'autres équipements sur le même réseau, usage du poste à des fins non professionnelles).
- **Compromission de l'activité :** En ces temps de crise sanitaire, l'activité des entités est davantage tributaire de leurs systèmes d'information. Les attaquants chercheront par tous les moyens à porter atteinte au bon fonctionnement de ces systèmes, notamment à travers des attaques de déni de service. A ce titre, les services en ligne et les plateformes d'accès distant sont les plus visés par ce type d'attaques.

Pour arriver à leurs fins, les principaux moyens et vecteurs d'attaques utilisés sont :

- **L'hameçonnage (phishing)** : Il s'agit de messages frauduleux (email, SMS, chat…) visant à dérober des informations confidentielles (mots de passe, données sensibles de l'entité, informations personnelles ou bancaires) en usurpant l'identité d'un tiers de confiance ou infecter la machine par des codes malveillants (Virus, Ransomware, programme espion,..). Cette technique profite désormais d'une part de l'engouement autour de l'information relative à la pandémie COVID-19 et d'autre part de l'utilisation de la messagerie électronique comme moyen principal de communication entre collaborateurs.
- **Contournement des mécanismes d'accès aux systèmes d'information :** L'accès distant en l'absence de mesures de sécurité appropriées, augmente les possibilités d'accès aux systèmes d'information offertes aux attaquants. Cet accès, peut se faire directement en exploitant des insuffisances sur les systèmes et applications exposés sur Internet, ou indirectement en passant à travers un poste utilisateur compromis utilisé comme point de rebond.

B. MESURES DE PROTECTION LIEES AU TELETRAVAIL

Pour faire face aux risques précités, il est recommandé de mettre en œuvre les mesures de cybersécurité ci-après et d'attirer l'attention du RSSI pour veiller à leur application :

1. **Utiliser des moyens et équipements appropriés pour le télétravail** : Il est fortement recommandé de privilégier autant que possible l'utilisation de moyens, mis à disposition, sécurisés et maîtrisés par l'entité (dotés d'Antivirus, Firewall, cryptage des disques...) et de renforcer la sécurité d'accès aux systèmes d'information sensibles.
2. **Limiter les accès distants** : L'ouverture des accès extérieurs ou distants doit être réservée aux personnes et services indispensables, et faire strictement l'objet d'un filtrage au niveau du pare-feu. Ces accès doivent s'appuyer sur des privilèges adéquats et se limiter aux besoins des utilisateurs. Il convient aussi de cloisonner les systèmes pour lesquels un accès à distance n'est pas nécessaire pour les préserver.
3. **Sécuriser les accès distants** : Les connexions distantes aux systèmes d'information internes doivent systématiquement s'effectuer via un réseau privé virtuel (VPN). La mise en place d'une double authentification est à privilégier pour se prémunir de l'usurpation de l'identité.
4. **Renforcer la politique de mots de passe** : Les mots de passe doivent être suffisamment longs, complexes et uniques sur chaque équipement ou service utilisé. Dans ce contexte, Il convient aussi de réduire la durée de changement des mots de passes et implémenter des mécanismes pour contrecarrer des attaques par force brute. Au moindre doute ou même en prévention, il faut changer les mots de passe et activer la double authentification chaque fois que cela est possible.

5. **Veiller au respect du déploiement des mises à jour de sécurité** : Tous les équipements et systèmes et en particulier ceux qui sont exposés au réseau Internet (postes nomades, tablettes, smartphones, serveurs, équipements réseaux ou de sécurité…) doivent systématiquement et immédiatement bénéficier des mises à jour de sécurité. En effet, un défaut de mise à jour d'un seul équipement est souvent la cause d'une intrusion dans le réseau des entités.

6. **Veiller à la sauvegarde des données** : Ne disposant pas forcément des mécanismes de sauvegarde automatiques déployés au niveau central des entités, les télétravailleurs doivent être sensibilisés sur l'importance de sauvegarder eux même régulièrement leurs données afin de faire face à d'éventuelles pertes de données suite à une cyberattaque (Ransomware par exemple).

7. **Superviser l'activité des accès externes et systèmes sensibles** : Cette supervision doit permettre à l'entité de pouvoir détecter toute activité anormale qui pourrait être le signe d'une cyberattaque, tels une connexion suspecte d'un utilisateur inconnu, ou élévation des privilèges d'un utilisateur connu, ou encore un volume inhabituel de téléchargement d'informations…

8. **Activer la journalisation au niveau de l'infrastructure de télétravail :** La journalisation est souvent le seul moyen de pouvoir comprendre comment a pu se produire une cyberattaque et donc de pouvoir y remédier, ainsi que d'évaluer l'étendue de l'attaque. Aussi, il convient d'activer la journalisation notamment au niveau des postes nomades, des équipements périmétriques et des services exposés.

9. **Respecter les règles de sécurité au niveau des plateformes collaboratives**: L'usage des plateformes en Cloud pour l'échange d'informations professionnelles (Visio conférence, Partage de documents, messagerie, etc..) doit se faire en veillant à ne pas partager des données sensibles. En tout cas et autant que faire se peut, il est recommandé de recourir à des connexions VPN et à des mécanismes d'authentification forte.

10. **Sensibiliser et apporter un soutien aux télétravailleurs :** Il s'agit de Donner aux télétravailleurs des consignes claires sur ce qu'ils peuvent faire ou ne pas faire et les sensibiliser aux risques de sécurité liés au télétravail. Il convient d'attirer leur attention notamment sur :

    - L'usage exclusif des équipements de télétravail à des fins professionnelles ;
    - L'usage du protocole sécurisé (WPA2) et de mots de passes robustes pour protéger le réseau wifi à domicile ;
    - La déclaration systématique de tout incident ou événement suspect au RSSI de son entité.

Pour toute éventuelle assistance ou complément d'informations, veuillez contacter la DGSSI sur l'adresse électronique suivante : **contact@dgssi.gov.ma.**