Covid-19 : le ministère des Armées au rendez-vous du télétravail

Mise à jour : 18/05/2020 - Auteur : La Rédaction - Direction : DICoD

Le ministère des Armées a mis en œuvre, dès le début de la crise du Covid-19, un plan de continuité d'activité plaçant, notamment, un maximum de personnel en télétravail. Essentiel à la continuité des missions essentielles, ce recours massif au télétravail augmente aussi, *de facto*, les risques de cyberattaques à l'encontre des systèmes d'information interconnectés avec l'Internet. Sous l'impulsion du Commandement de la cyberdéfense - COMCYBER, le ministère est passé en posture de cyberdéfense « écarlate », son plus haut niveau d'alerte.

Le ministère s'est rapidement adapté. Grâce à la solution de mobilité SMOBI, une partie du personnel peut accéder, directement et en toute confiance, à l'Intradef (réseau interne du ministère), afin de poursuivre ses activités professionnelles. En quelques semaines, **le nombre d'utilisateurs de postes Intradef en télétravail a été multiplié par 3. Tout le personnel a donc dû faire l'objet d'un rappel aux règles de la cybersécurité**.

Officier traitant en protection et défense cyber au COMCYBER, le lieutenant-colonel Daniel souligne les défis auxquels est actuellement confronté le ministère des Armées : « *Nous distinguons le télétravail, c'est-à-dire l'utilisation de PC SMOBI permettant un accès sécurisé à l'Intradef, et le travail à domicile qui s'effectue avec des moyens personnels (ordinateur familial, clé USB personnelle). Ces outils présentent des vulnérabilités et offrent donc des opportunités d'attaques aux cybercriminels. Leur utilisateur peut être victime de phishing, de vol de données, de virus...* ***Le personnel du ministère des Armées doit bien être conscient que cette situation transitoire et exceptionnelle nécessite une extrême prudence.*** *Chacun sait que l'interconnexion d'équipements professionnels avec des moyens personnels (clé USB ou disque dur externe) fragiliserait ces équipements professionnels, voire le réseau Intradef dans son ensemble, lorsque l'agent revient à son poste de travail et reconnecte son PC portable. Nous avons rappelé à notre personnel de ne prendre aucun risque et de bien séparer les deux domaines.* »

Car l'enjeu est de taille. « *La cybersécurité est l'affaire de tous »,* rappelle l'officier. *« **Il suffit d'une machine infectée pour qu'un réseau entier soit compromis.** Nous avons ainsi mis en place au sein du COMCYBER une adresse mail dédiée permettant aux personnes de nous solliciter directement en cas de doutes. Par ailleurs, nous les orientons vers le site* secnumacademie.gouv.fr *dont les nombreux contenus pédagogiques permettent d'approfondir les connaissances de chacun en cybersécurité et ainsi mieux protéger ses outils numériques personnels.* »

Les menaces n'ont pas disparu

Le 11 mai représente un nouveau défi avec la mise en place du plan de reprise progressive de l'activité du ministère des Armées. Les solutions de télétravail sont encore encouragées, mais une partie du personnel reprend progressivement au sein des emprises du ministère, rendant indispensables les mesures de vigilance cyber. « *Lors du déconfinement, si le personnel a travaillé depuis chez lui avec son équipement professionnel, il doit impérativement le faire contrôler avant de le reconnecter au réseau interne.* », précise le lieutenant-colonel Daniel.

Comment éviter les erreurs ? Comment protéger ses données ? Le ministère des Armées recommande à son personnel d'adopter les bonnes pratiques pour garantir la sécurité du réseau.

Voir l'infographie : « Les 10 commandements cyber »

Malware, rançongiciel, hameçonnage… L'application de bonnes pratiques – dites « d'hygiène cyber » - permet à tout utilisateur de se prémunir contre les actes malveillants sur Internet. Les actes cyber-malveillants sont en augmentation du fait de la crise sanitaire liée à l'épidémie du Covid-19 et le télétravail augmente l'exposition du ministère des Armées aux menaces cyber.

Voir le tuto : cybersécurité, trois bons réflexes