Télétravail et SSI

Un challenge quotidien

Michel **CHABANNE** – RSSI-C – CNRS

michel.chabanne@cnrs.fr | @SSiCnrs | https://securite-si.cnrs.fr

19/11/2020 – IN2P3

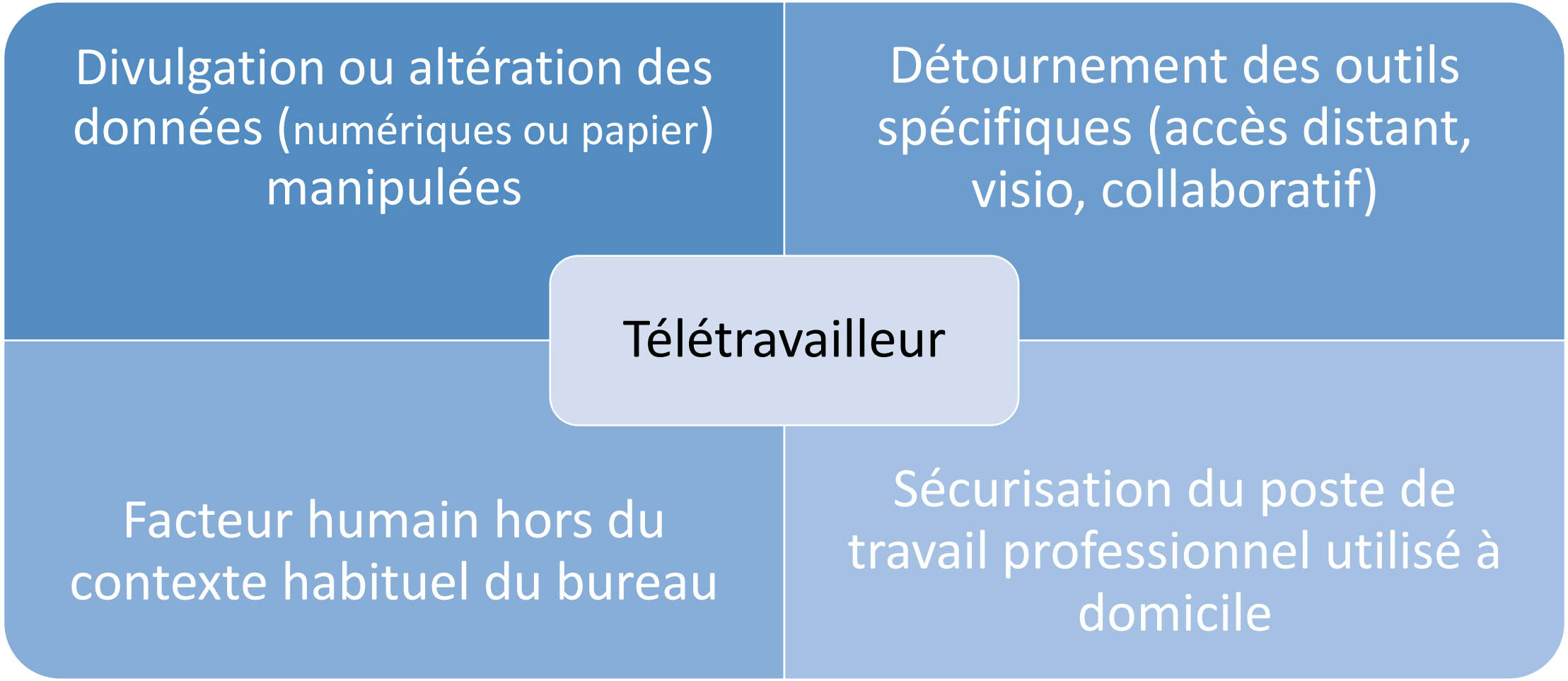
Télétravail (TW): des expérimentations à la massification

- Décret n° 2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique (modifié Décret n° 2020-524 du 5 mai 2020 > « *FlexOffice* »)
- Mise en œuvre au CNRS : 01/01/2019, 3000 agents en 2019
  - Note d'organisation DRH
  - Guide de mise en œuvre
- Grèves de transport en RP fin 2019 puis crise COVID-19
  - Extension du télétravail « imposé » par l'Etat liée au(x) confinement(s)
  - Massification de certains usages : visioconférence, accès distant
- Quels impacts pour la sécurité des SI ?

Rappels sur les consignes de mise en oeuvre

- Identification de **tâches non télétravaillables** (hors contexte spécifique COVID)
- Utilisation d'un **lien réseau sécurisé** pour l'accès au SI unité
- Validation de la conformité SSI du **poste de travail professionnel**
- Usage exclusif du poste de travail professionnel
- Renvoi du poste téléphonique pro à domicile
- Utilisation préférentielle d'un réseau local filaire
- Usage **d'outils d'échange (a)synchrones validés** par l'établissement
  - Outils collaboratifs (Core, myCore)
  - Visioconférence (Tixeo, myCom, Renavisio/Rendez-vous)
  - VPN (fourni par l'unité)

Risques du TW massif



Les incidents au CNRS liés au TW

- Usage illicite de postes de travail personnels
- Non-conformité des passerelles d'accès distant
- Exposition trop large de ressources (avec ou sans VPN)
- Usage d'outils non conformes aux instructions de la tutelle (extension du *shadow IT*)
- Défacement de sites web dont l'administration a été trop largement ouverte suite au confinement
- Transport non sécurisé de données au format papier
- Vagues de phishing opportunistes lié à la dématérialisation « forcée » et mal encadrée des processus (faux liens Onedrive, fausses signatures…)
- Attaques dirigées vers les unités actives sur la recherche sur COVID-19

Les actions de l’ASR d’unité en TW

- S’assurer de la maintenance de son infrastructure (mise à jour, revue des configurations) : accès distant, outils métiers mis à dispo, postes de travail
- Surveiller ses infrastructures, à la recherche d’indicateurs de compromission
- Gérer les ouvertures de flux de manière parcimonieuse et temporaire
- Sensibiliser les utilisateurs aux risques récurrents (notamment liés aux téléprocédures), à la sauvegarde des données
- Ne pas négliger les postes de travail: chiffrement, pare-feu, antivirus, …
- Attention à l’administration à distance ! (bastion/serveur rebond)
- Remonter les incidents à la chaîne fonctionnelle SSI

Bibliographie

- (CNRS) Guide opérationnel CNRS
- https://intranet.cnrs.fr/Cnrs_pratique/recruter/_layouts/15/WopiFrame.aspx?sourcedoc=/Cnrs_pratique/recruter/Documents/guide-operationnel-teletravail.pdf&action=default&DefaultItemOpen=1
- (CNRS) Bonnes pratiques
- https://intranet.cnrs.fr/delegations/dr16/delegation/_layouts/15/WopiFrame.aspx?sourcedoc=/delegations/dr16/delegation/Documents/T%C3%A9l%C3%A9travail%20Les%20bonnes%20pratiques.pdf&action=default&DefaultItemOpen=1
- Cybermalveillance: TW en situation de crise
- https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail
- ANSSI: Nomadisme numérique
- https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf