Télétravail 101 – les mesures à mettre en place par un organisme public

Type : Recommandation (pratique)
Référence légale : LGGRI, chapitre G-1.03, 12(6)
Statut : En vigueur
Numéro de référence : P_2020_012
Dernière mise à jour : 2021-05-31
Remplace • P_2020_003 « Télétravail et sécurité de l'information »

Champ d'application

Organismes (OP) visés à l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics (chapitre G-1.03).

Voici quelques actions que les organismes peuvent mettre en place afin d'atténuer les risques associés au télétravail quant à la sécurité de l'information (serveurs et communications d'accès à distance, postes de télétravail, etc.) :

- Éviter d'exposer directement à Internet son réseau organisationnel. Mettre à la disposition du personnel un point d'accès contrôlé, dans une zone sécurisée, en utilisant un des mécanismes recommandés pour lui offrir une connexion à distance[(1)] sécuritaire.
- S'assurer que les serveurs d'accès à distance sont sécurisés efficacement et maintenus à jour.
- Exiger une authentification multifacteur (« MFA ») pour l'accès aux infrastructures de l'organisme (SMS_2020_004 Authentification multifacteur (« MFA ») pour les accès réalisés à partir d'Internet).
- Assurer le chiffrement du canal de communication en tout temps. Il peut s'agir, par exemple, de la mise en place d'un réseau privé virtuel (« VPN ») ou d'une communication chiffrée (de type HTTPS) entre le poste de télétravail et le réseau de l'organisme.
- Limiter l'accès aux données essentielles en imposant un contrôle auprès des télétravailleuses et télétravailleurs.
- Disposer d'un registre des accès aux différents services et données et le maintenir à jour.
- Journaliser les accès aux différents services, notamment aux réseaux privés virtuels (« VPN ») (SMS_2020_008 Surveillance continue des authentifications).
- Sécuriser tous les types d'appareils de télétravail, y compris les ordinateurs de bureau et portables, les téléphones intelligents et les tablettes numériques, contre les menaces courantes (SMS_2020_003 Solution antivirus avec fonctionnalités d'Endpoint Detection and Response (EDR)).
- S'assurer que l'information conservée sur le poste de travail est chiffrée (BitLocker, FileVault ou un équivalent, selon système d'exploitation).
- Bloquer l'accès à toute boîte de courriels non attribuée par l'organisme (P_2020_006 Boîtes de courriels non attribuées par l'organisme).
- Déterminer si le personnel est appelé à travailler avec des données confidentielles et évaluer les répercussions en cas de violation de la confidentialité.

Pour obtenir de l'aide à l'interprétation de ce document, contactez votre centre opérationnel de cyberdéfense ou le centre gouvernemental de cyberdéfense (cgcd@mcn.gouv.qc.ca).

- Indiquer au personnel les mesures à prendre en cas d'activités problématiques sur un appareil de télétravail (par exemple : déconnecter le poste de télétravail du réseau) et fournir aux utilisatrices et utilisateurs les coordonnées pour joindre le centre de services (SMS_2020_013 Consignes en cas de menaces potentielles ou avérées).
- Mettre en place une directive interne sur le télétravail, qui précise notamment :
    - si l'utilisation des assistants numériques personnels est permise,
    - les niveaux d'accès à distance autorisés, selon le type d'appareils.

  Par exemple, un organisme pourrait décider que les ordinateurs dont il est propriétaire aient accès à de nombreuses ressources, alors que l'accès des assistants numériques personnels des employées et employés seraient limités à celles qui représenteraient un faible risque (comme le courriel Web).
- Proscrire l'utilisation de postes de travail personnels. Si une telle interdiction n'est pas envisagée, il est essentiel que l'organisme :
    - mette en place des mécanismes de sécurité appropriés, comme un réseau privé virtuel (« VPN SSL ») qui permet exclusivement un accès à des outils de connexion à distance (Citrix, Terminal Server, etc.);
    - active des fonctionnalités qui assurent une conformité minimale aux exigences de sécurité, avant d'autoriser le branchement d'un poste personnel à son réseau (antivirus à jour, version du système d'exploitation reconnue, etc.);
    - obtienne l'autorisation de sa dirigeante ou de son dirigeant. Comme prévu à la Directive sur la sécurité de l'information gouvernementale, une gestion adéquate des risques doit être réalisée pour que cette prise de décision soit appuyée.

Mécanismes pour une connexion à distance sécuritaire du personnel

- Le **réseau privé virtuel** (« VPN ») consiste à l'établissement d'un canal de communication sécurisé entre un poste de télétravail et un serveur d'accès distant. Les communications qui transitent par ce canal sont cryptées afin que leur confidentialité et leur intégrité soient protégées. Les canaux peuvent également servir à authentifier les utilisatrices et utilisateurs. De plus, l'accès des postes de travail aux systèmes de l'organisme peut être contrôlé, voire restreint. Les types de réseaux privés virtuels les plus couramment utilisés pour le télétravail emploient les protocoles IPsec et SSL (Secure Sockets Layer).
- Le **portail** est un serveur qui agit comme un intermédiaire entre une ou plusieurs applications et les postes de télétravail de l'organisme, et ce, par une seule interface centralisée. Les communications entre les postes de télétravail et les applications sont alors protégées. Les portails peuvent également authentifier les utilisatrices et utilisateurs et restreindre l'accès aux ressources internes de l'organisme. Parmi les mesures supplémentaires, il est possible de bloquer les fonctionnalités de presse-papier et de partages de ressources du poste en télétravail.
- **L'accès direct aux applications** permet au personnel d'utiliser directement, à partir de son poste de télétravail, les applications situées sur le réseau interne de l'organisme, et ce, sans avoir recours à un logiciel à cette fin. Les applications peuvent s'appuyer sur leurs propres mécanismes de sécurité (chiffrement des communications, authentification des utilisateurs, etc.). Le courriel Web est un exemple d'accès direct aux applications. Généralement, l'accès direct aux applications

ne doit être utilisé que dans des cas exceptionnels et après le déploiement de mesures de mitigation adéquates qui s'appuient sur une analyse minutieuse des risques de sécurité.

- L'**accès au bureau à distance** permet au personnel de contrôler un ordinateur particulier au sein de l'organisme, le plus souvent le sien, à partir d'un poste de télétravail. Le personnel contrôle les périphériques d'entrée (par exemple, le clavier et la souris) sur l'ordinateur distant, et l'écran est visible sur celui de son poste de télétravail. Généralement, l'accès au bureau à distance ne doit être utilisé que dans des cas exceptionnels et après le déploiement de mesures de mitigation adéquates qui s'appuient sur une analyse minutieuse des risques de sécurité.

Voir aussi

Guide d'utilisation sécuritaire des assistants numériques personnels
P_2020_006 Boîtes de courriels non attribuées par l'organisme
P_2020_013 Télétravail 101 – les mesures à suivre par le personnel
SMS_2020_003 Solution antivirus avec fonctionnalités d'Endpoint Detection and Response (EDR)
SMS_2020_004 Authentification multifacteur (« MFA ») pour les accès réalisés à partir d'Internet
SMS_2020_008 Surveillance continue des authentifications
SMS_2020_013 Consignes en cas de menaces potentielles ou avérées