Lettre Cyber 67

Septembre / Octobre 2022

La sécurisation du télétravail

Aujourd'hui il paraît évident de protéger son système d'information au sein de son entreprise ou de sa collectivité notamment. L'histoire récente a vu le développement accrue du télétravail qui présente de réelles opportunités. Il nécessite toutefois généralement l'ouverture vers l'extérieur du système d'information de l'organisation. Cela implique parfois l'emploi de matériel personnel pour se connecter à un réseau professionnel. Voici 10 recommandations à mettre en œuvre pour limiter au mieux les risques.

1/ Définissez et mettez en œuvre une politique d'équipement des télétravailleurs : Privilégiez autant que possible l'utilisation de moyens mis à disposition, sécurisés et maîtrisés par votre organisation. Lorsque ce n'est pas possible, donnez des directives d'utilisation et de sécurisation claires aux employés en ayant conscience que leurs équipements personnels ne pourront jamais avoir un niveau de sécurité vérifiable (voire sont peut-être déjà compromis par leur usage personnel).

2/ Maîtrisez vos accès extérieurs: Limitez par un pare-feu l'ouverture de vos accès extérieurs ou distants (RDP par exemple) aux seules personnes et services indispensables, et filtrez strictement ces accès grâce à cet équipement de sécurité. Une attention toute particulière sera portée sur les éventuels accès de télémaintenance qui peuvent présenter une vulnérabilité importante s'ils sont compromis. Cloisonnez également les systèmes pour lesquels un accès à distance n'est pas nécessaire pour les préserver, surtout s'ils revêtent un caractère sensible pour l'activité de votre organisation (comme les réseaux de sauvegardes et les réseaux d'administration informatique).

3/ Sécurisez vos accès extérieurs: Systématisez les connexions sécurisées à vos infrastructures par l'utilisation d'un « VPN » (*Virtual Private Network* ou « réseau privé virtuel » en français). Outre le chiffrement de vos connexions extérieures, ces dispositifs permettent également de renforcer la sécurité de vos accès distants en les limitant aux seuls équipements authentifiés. La mise en place d'une double authentification sur ces connexions VPN sera également à privilégier pour se prémunir de toute usurpation.

4/ Renforcez votre politique de gestion des mots de passe: Qu'il s'agisse des mots de passe des utilisateurs en télétravail, mais aussi de ceux en charge du support informatique, les mots de passe doivent être suffisamment longs, complexes et uniques sur chaque équipement ou service utilisé. Les mots de passe doivent être changés régulièrement et, autant que possible, associés à une double authentification.

5/ Ayez une politique stricte de déploiement des mises à jour de sécurité: Les mises à jour permettent notamment de corriger une faille découverte. Elles sont donc à réaliser dès qu'elles sont disponibles sans tarder. En effet les pirates mettent peu de temps à exploiter ces failles. Un défaut de mise à jour est souvent la cause d'une intrusion dans le réseau des organisations. Elles concernent aussi bien les matériels que les logiciels. D'où l'importance de sécuriser son matériel personnel aussi bien que son matériel professionnel.

Recevoir cette lettre info par mail, envoyez-nous votre demande :
arnaud.schweitzer@gendarmerie.interieur.gouv.fr ou mathieu.knobloch@gendarmerie.interieur.gouv.fr

La sécurisation du télétravail

6/ Durcissez la sauvegarde de vos données: La sauvegarde est un point essentiel à respecter afin de pouvoir recouvrer ses données à la suite d'une cyberattaque. Il convient donc de vérifier que le service souscrit par l'utilisateur d'un poste nomade ou pour un hébergement externe (cloud par exemple) puisse assurer un niveau de sécurité et de récupération des sauvegardes suffisant selon les risques encourus par votre organisation. Il convient également de s'assurer du niveau de sauvegarde **des données des postes nomades des collaborateurs et de celles de ses hébergements externes** (cloud, site Internet de l'organisation, service de messagerie…) pour vérifier que le service souscrit est bien en adéquation avec les risques encourus par votre organisation

7/ Utilisez des solutions antivirales professionnelles: Ces solutions permettent de protéger les organisations de la plupart des attaques virales connues, mais également parfois des messages d'hameçonnage (*phishing*), voire de certains rançongiciels (*ransomware*). Utiliser des solutions différentes pour la protection des infrastructures et pour les terminaux peut s'avérer complémentaire et démultiplier ainsi l'efficacité de la protection dans un principe de défense en profondeur.

8/ Mettez en place une journalisation de l'activité de tous vos équipements d'infrastructure: Ayez une journalisation systématique et d'une durée de rétention suffisamment longue de tous les accès et activités de vos équipements d'infrastructure (serveurs, pare-feu, proxy…), voire des postes de travail. Cette journalisation sera 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.

9/ Supervisez l'activité de vos accès externes et systèmes sensibles: Cette supervision doit vous permettre de pouvoir détecter le plus rapidement possible toute activité anormale qui pourrait être le signe d'une cyberattaque, telle une connexion suspecte d'un utilisateur inconnu ou d'un utilisateur connu en dehors de ses horaires habituels, ou encore un volume inhabituel de téléchargement d'informations…

10/ Sensibilisez et apportez un soutien réactif à vos collaborateurs en télétravail: Donnez aux télétravailleurs des consignes claires **et formalisées** sur ce qu'ils peuvent faire ou ne pas faire et sensibilisez-les aux risques de sécurité liés au télétravail. Cela doit se faire avec pédagogie pour vous assurer de leur adhésion et donc, de l'efficacité des consignes. Les utilisateurs sont souvent le premier rempart pour éviter, voire détecter les cyberattaques.