Télétravail: Sécuriser son accès à distance

NCSC

Version:	v 1.0
Auteur:	NCSC
Dernière mise à jour:	24 mars 2020

Introduction

Etant donné l'utilisation accrue des solutions d'accès à distance pour le télétravail, il est opportun de rappeler les bonnes pratiques afin de minimiser le risque lié à ces technologies. Nous sommes convaincus que ce dernier augmente avec l'accroissement des différentes connexions à distance. Des attaquants sont informés de cette situation et tentent, par différents moyens, de gagner accès au réseau des organisations:

- Des tentatives de phishing (qu'elles soient classiques pour l'obtention de mots de passe ou en temps réel[1] dans les cas d'authentification à deux facteurs)
- Attaques contre les mots de passe (attaque de dictionnaire, password spaying ou encore des attaques de brute force)
- Attaques contre les systèmes de gateways non-patché
- Via des maliciel (qui restent souvent non détectés si une tunnellisation de l'ensemble du trafic n'est pas en place).

Contremesures

Considérations quant à la capacité

La mise en place du télétravail peut amener à une augmentation importante des besoins en bande passante. Il est conseillé d'en discuter avec votre fournisseur de télécommunication et votre équipe interne. Cependant, cette augmentation à elle seule n'est pas suffisante. En effet les appareil dits *downstream* tels que les pare-feu, les systèmes anti-intrusion mais aussi les switches et les serveurs pourraient devenir surchargés si leurs capacités ne sont pas elles aussi adaptées.

Mesures contre les maliciels et le phishing

- Toujours utiliser une authentification forte, c'est-à-dire avec au moins **deux facteurs d'authentification** pour vos utilisateurs. La meilleure option serait un facteur matériel tel une clé USB ou une smartcard ou encore un system de OTP ("*One Time Password*") matériel tel que RSA ou encore MobilleID. Si cela n'est pas possible, un facteur logiciel tel qu'un token OTP avec par exemple Google Authenticator est aussi recommandé
- Mettre en œuvre et faire respecter les **bonnes pratiques en matière de mots de passe**. Il faut notamment veiller à ce que les mots de passe ne soient pas réutilisés

[1] Voir Rapport semestriel 2019/1, chap. 4.4.2, https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/halbjahresbericht-2019-1.html.

pour différents services et que les utilisateurs n'utilisent pas de séquences (p. ex. xyz2018, xyz2019, xyz2020)

- **Surveiller les logs des accès à distance** pour identifier toute anomalie (p.ex. des adresses IP suspectes, venant de l'étranger alors que votre force de travail est basée en Suisse, des adresses venant de sorties TOR ("*Exit-Nodes*"), de services VPN et de manière générale venant de réseaux de fournisseurs d'hébergement)
- **Appliquer un tunnel VPN** pour tous les appareils afin de garantir la sécurité des communications et maintenir une visibilité des connexions en direction de l'Internet. Gardez à l'esprit que cette mesure augmentera significativement vos besoins en bande passante
- **Informez vos utilisateurs des dangers** du télétravail et fournissez-leur un **point de contact** unique en cas d'activité suspecte
- Ayez des **plans d'analyse forensique** en place, notamment si les collaborateurs sont autorisés à utiliser leurs appareils pour accéder aux ressources de l'entreprise.
- Assurez-vous que tous les **appareils** d'accès à distance soient **à jour** et définissez **un plan de mise-à-jour d'urgence** ("*emergency patch roll-out*") en cas de vulnérabilité critique
- Assurez-vous que les appareils puissent être mis à jour sans être physiquement sur place, de préférence en dehors de heures de travail, et avec la bande passante disponible
- Assurez-vous que les utilisateurs de télétravail n'interconnectent pas leur **réseau privé** (du domicile) avec celui de l'entreprise
- Planifiez la remise à niveau et le *remote staging* d'**appareils infectés**, p.ex. via une lignes DSL/fibre dédiée.

En plus de ces recommandations, nous vous signalons les documents relatifs à la protection contre les rançongiciels ciblés que nous avons publiés récemment:

- https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes
- https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/sicherheitsrisiko-durch-ransomware.html
- https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/assets/blocked-filetypes.txt

Sécurité des données

- Assurez-vous que vous avez des **sauvegardes hors-ligne** en cas de rançongiciel
- Assurez-vous que des solutions de sauvegarde soient en place et efficaces si les utilisateurs **enregistrent des données importantes localement**
- Si l'usage des appareils personnels (**BYOD**) augmente, assurez-vous que vous avez des **lignes directrices de base pour ces appareils**, que les données appartenant à

votre organisation puissent être enregistrées de manière sûre (par exemple dans un container chiffré) et que ces dernières puissent être effacées efficacement si par exemple l'utilisateur veut revendre son appareil. Pour rappel, les données enregistrées sur des SSD non-chiffrés requièrent un effort supplémentaire pour être effacées.

Sensibilisation

- Mettez en arrêt toutes les **campagnes de sensibilisation** au phishing afin de réduire les perturbations
- Informez vos utilisateurs concernant les **risques additionnels** et demandez-leur de signaler tout courriel ou site web suspect à votre helpdesk
- Assurez-vous que votre **helpdesk est suffisamment équipé** en ressources
- Formez vos utilisateurs à la **sécurisation des réseaux WiFi**
- Informez vos utilisateurs des **moyens de contacter le helpdesk** et dites leur comment celui-ci peut les contacter afin d'éviter les fraudes au soutien ("support scam")[2]
- Mettez en place une **méthode d'authentification** simple en cas de réinitialisation des mots de passe.

Divers

- **Documentez tous les changements** durant la situation d'urgence afin de pouvoir revenir à la normale lorsque la situation le permet
- Assurez-vous que les **tâches administratives** qui requièrent des privilèges élevés soient exécutées depuis des **appareil sécurisés** qui ne peuvent pas accéder à Internet en même temps. Utilisez des instances de terminal de serveur dédiées si possible
- Si vous observez des **tentatives de phishing** ou des **activités de maliciels**, annoncez-les sur www.antiphishing.ch .
- **Renseignez-vous** sur l'état de la menace cyber actuelle uniquement par des sources sûres tels que https://www.ncsc.ch, https://www.govcert.ch, https://twitter.com/GovCERT_CH, https://www.bsi.bund.de/DE/Home/home_node.html, https://www.ssi.gouv.fr/
- Facilitez les **demandes de fonctionnalités et d'outils** ("*feature and tool request*") à votre service desk. Si vous ne pouvez pas offrir une solution interne, il est recommandé d'offrir des instructions quant à des solutions tierces afin de minimiser les solutions de rechanges individuelles qui sont impossibles à surveiller.

[2] Appels d'escrocs: https://www.melani.admin.ch/melani/fr/home/themen/fake_support.html.

Résumé

La gestion de risque et la sécurité opérationnelle devraient s'adapter rapidement à la nouvelle surface d'attaque actuelle. Des contre-mesures appropriées devraient être implémentées notamment pour les risques considérés comme critiques. Nous recommandons d'éviter des changements complexes dans la situation actuelle, mais plutôt de réduire les risques en augmentant les la capacité de détection. Si vous avez des questions, n'hésitez pas à nous contacter sur outreach[at]ncsc.ch.