Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Secrétariat général

Centre national pour la cybersécurité NCSC
www.ncsc.admin.ch

NCSC

Télétravail

Sécuriser son accès à distance

Table des matières

1 Introduction

Les entreprises utilisent de plus en plus les possibilités d'accès à distance à leur réseau. L'utilisation de ces technologies augmente toutefois le risque de cyberattaques.
Les cybercriminels utilisent les procédés les plus variés pour accéder aux réseaux d'entreprise:

- tentatives d'hameçonnage (qu'elles soient classiques dans le but d'obtenir un mot de passe ou «en temps réel[1]» dans les cas de l'authentification à deux facteurs);
- attaques de mots de passe (attaques contre des services d'annuaire, modifications de mots de passe ou encore attaques par force brute);
- attaques contre des passerelles (*gateway*) non sécurisées;
- attaques à l'aide de maliciels (qui ne sont généralement pas détectés sans l'installation d'un tunnel pour l'ensemble du trafic).

2 Contre-mesures

2.1 Considérations avant l'utilisation de logiciels d'accès à distance

L'utilisation de logiciels d'accès à distance doit faire l'objet d'une analyse attentive car elle peut provoquer une augmentation importante de la charge sur la bande passante. Il est conseillé d'en discuter avec son fournisseur d'accès à Internet et son équipe interne de spécialistes en informatique. Une augmentation de la bande passante n'est pas suffisante si les systèmes en aval (pare-feu, systèmes anti-intrusion, commutateurs réseau, serveurs, etc.) ne peuvent pas traiter l'augmentation du flux de données.

2.2 Protection contre les maliciels et l'hameçonnage

- Utilisez toujours un **deuxième facteur** pour **l'authentification de l'utilisateur**. Les clés de sécurité, les smartcards ou tout autre matériel informatique qui génère un mot de passe à usage unique (o*ne time password, OTP*) tels que les jetons RSA ou MobileID représentent de bonnes solutions. Si de telles solutions ne sont pas envisageables, une solution logicielle telle que Google Authenticator est aussi adaptée.
- Imposez **l'utilisation de mots de passe forts** et rappelez aux utilisateurs de définir un mot de passe différent pour chaque service et d'éviter les séquences (par ex. password1, password2, etc.).
- Surveillez constamment les données de journal de vos appareils utilisés pour l'accès

[1] Voir MELANI, rapport semestriel 2019/1, chap. 4.4.2, https://www.ncsc,admin.ch/ncsc/fr/home/dokumentation/berichte/lageberichte.html

à distance afin de détecter toute anomalie (par ex. des adresses IP étrangères alors que la plupart des collaborateurs travaillent en Suisse; adresses IP des réseaux Tor; VPN ou réseaux de fournisseurs d'hébergement).

- Imposez un **tunnel** à tous les appareils afin de garantir la sécurité des communications et la protection de la visibilité des connexions sur Internet. Gardez à l'esprit que cette mesure augmentera significativement la charge sur la bande passante.
- **Sensibilisez** vos **collaborateurs** aux cybermenaces, notamment dans le cadre du travail à domicile, et fournissez des **informations de contact** au cas où un collaborateur détecterait une activité suspecte.
- Préparez des **plans d'analyse forensique**, notamment si vous autorisez vos collaborateurs à accéder à votre réseau d'entreprise avec leurs appareils personnels.
- Vérifiez que tous les appareils utilisés pour l'accès à distance sont **à jour** (correctifs) et définissez un **plan de mise à jour d'urgence** en cas de faille critique de sécurité.
- Assurez-vous que la mise à jour des appareils utilisés pour l'accès à distance ne nécessite pas la présence des collaborateurs dans les locaux de l'entreprise.
- Assurez-vous que les personnes qui travaillent à domicile ne **peuvent pas établir de connexion** entre leur **réseau domestique** et le **réseau d'entreprise**.
- Planifiez la réinitialisation/le remplacement des **appareils infectés** à distance, par ex. via une ligne DSL/fibre optique dédiée.
- En plus de ces recommandations spécifiques, observez les mesures de protection[2] contre les rançongiciels publiées par le NCSC.

2.3 Sécurité des données

- Assurez-vous de posséder des **sauvegardes hors-ligne** en cas de d'attaque par un rançongiciel.
- Assurez-vous que des solutions de sauvegarde sont en place et sont efficaces si les utilisateurs **enregistrent localement des données importantes**.

Si l'utilisation d'appareils personnels (*bring your own device*, **BYOD**) augmente, assurez-vous d'avoir des **instructions pour l'utilisation** de ces appareils. Les données appartenant à votre organisation doivent notamment être enregistrées en toute sécurité (par ex. dans un dossier chiffré) de sorte qu'elles puissent être effacées intégralement (*wiping*), notamment si l'utilisateur veut revendre son appareil. Gardez à l'esprit que la suppression complète de données enregistrées sur des disques durs non chiffrés demande beaucoup de manipulations supplémentaires.

[2] https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/
https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/news/news-archiv/sicherheitsrisiko-durch-ransomware.html
https://www.govcert.ch/blog/severe-ransomware-attacks-against-swiss-smes/assets/blocked-filetypes.txt

2.4 Sensibilisation

- Arrêtez toutes les **campagnes de sensibilisation à l'hameçonnage** afin de réduire l'agitation.
- Informez vos collaborateurs des **risques additionnels** et demandez-leur de signaler tout courriel ou site Web suspect à votre service d'assistance.
- Assurez-vous que votre **service d'assistance** dispose de suffisamment de personnel.
- Assistez vos collaborateurs dans la configuration de **réseaux sans fil sécurisés**.
- Informez vos collaborateurs des **solutions pour prendre contact avec le service d'assistance** et expliquez-leur comment ce dernier prendra contact avec eux afin d'éviter qu'ils ne soient victimes d'appels d'assistance frauduleux[3].
- Mettez en place une procédure simple pour **identifier les utilisateurs** qui demandent à réinitialiser leur mot de passe.

2.5 Divers

- **Documentez tous les changements** que vous avez initiés afin que ceux-ci puissent être annulés facilement si nécessaire.
- Assurez-vous que les **tâches administratives** qui requièrent des privilèges élevés soient exécutées uniquement depuis des **appareils sécurisés** qui ne peuvent pas accéder à Internet simultanément. Utilisez dans la mesure du possible des instances de serveur dédiées.
- Si vous observez des **tentatives d'hameçonnage** ou des **activités de programmes malveillants**, annoncez-les sur www.antiphishing.ch.
- Utilisez uniquement des sources **fiables**[4] pour vous renseigner sur les cybermenaces.
- Facilitez les **demandes en fonctionnalités et en outils** en cas d'urgence. Si vous ne pouvez pas offrir de solution interne, indiquez au minimum des solutions alternatives afin d'éviter que vos collaborateurs cherchent eux-mêmes des solutions qui seraient impossibles à surveiller.

2.6 Résumé

La gestion des risques et la sécurité opérationnelle exigent une adaptation rapide à l'évolution des menaces ainsi que des contre-mesures appropriées aux risques considérés comme hautement critiques. Nous recommandons d'éviter les changements complexes dans la situation actuelle et de réduire les risques en augmentant la capacité de détection. Si vous avez des questions, n'hésitez pas à nous contacter sur outreach[at]ncsc.ch.

[3] https://www.ncsc.admin.ch/ncsc/fr/home/cyberbedrohungen/fake-support.html

[4] https://www.ncsc.ch; https://twitter.com/GovCERT_CH; https://www.bsi.bund.de/DE/Home/home_node.html; https://www.ssi.gouv.fr/ etc.