Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 13 janvier 2017

N° DAT-NT-004/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 8

Note technique

Recommandations de sécurité relatives à la télé-assistance

Public visé :

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	✓

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les **« Recommandations de sécurité relatives à la télé-assistance »**. Il est téléchargeable sur le site www.ssi.gouv.fr. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Personnes ayant contribué à la rédaction de ce document :

Contributeurs	Rédigé par	Approuvé par	Date
BAI, BSS	BSS	SDE, Comité éditorial	13 janvier 2017

Évolutions du document :

Version	Date	Nature des modifications
1.0	7 septembre 2012	Version initiale
1.1	13 janvier 2017	Corrections et mises à jour mineures

Pour toute question :

Contact	Adresse	@mél
Bureau Communication de l'ANSSI	51 bd de La Tour-Maubourg 75700 Paris Cedex 07 SP	conseil.technique@ssi.gouv.fr

Table des matières

1 Préambule

L'utilisation croissante des technologies de l'information en perpétuelle évolution apporte des fonctionalités de plus en plus riches au niveau du poste de travail et, souvent, un usage de ce dernier propre à chaque individu. Il en résulte un besoin prégnant d'assistance des utilisateurs de manière à résoudre les problèmes qu'ils peuvent rencontrer sur leurs postes.

Par manque de ressources humaines et parce que les technologies employées le permettent, les services informatiques y répondent dans la majorité des cas par des opérations réalisées à distance. Force est de constater que la sécurité n'est pas toujours bien appréhendée pour réaliser ce type d'intervention alors que les solutions utilisées apportent des vulnérabilités et octroient aux intervenants des droits importants.

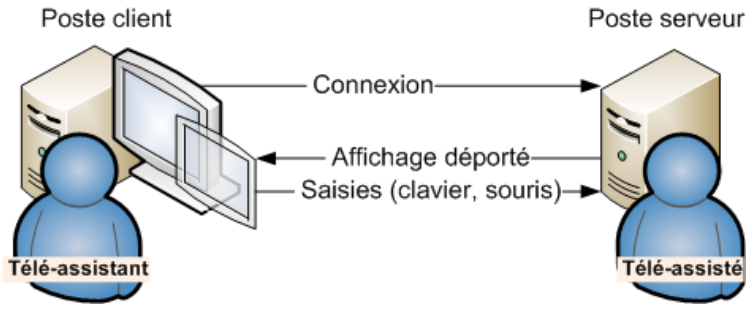

FIGURE 1 – Télé-assistance

Liste des recommandations

2 Les risques de sécurité des outils de télé-assistance

Par nature, un outil de télé-assistance donne un accès très large aux ressources disponibles sur le poste de travail d'un utilisateur. Ainsi, tout individu accédant à distance à un poste de travail lors d'une opération de télé-assistance peut prendre connaissance de l'ensemble des informations stockées sur la machine dont les données personnelles, utiliser différents périphériques qui y sont connectés (microphone, webcam etc.) voire employer les différentes applications installées en lieu et place des personnes se connectant localement. Se posent alors des problèmes de protection et de préservation de la confidentialité des informations contenues dans le poste de travail, de traçabilité des opérations réalisées et du contrôle par l'utilisateur des opérations effectuées sur sa machine.

En outre, l'accès illégitime par des personnes non autorisées aux traces laissées par l'utilisation de tels outils ou au canal établi entre le client et le serveur lors des opérations de télé-assistance augmente les risques de fuite d'informations sensibles, dont certaines pourraient être réutilisées pour accéder à d'autres ressources du système d'information encore plus critiques. Ainsi, si un mot de passe unique est utilisé pour les opérations de télé-assistance et d'administration du système d'information, sa récupération, par exemple par une attaque de « l'homme du milieu » [1], ouvrira de nombreuses autres possibilités à un individu mal intentionné.

Les solutions disponibles pour la télé-assistance ont évolué pour être aujourd'hui très riches fonctionnellement, souvent au détriment de la prise en compte de la sécurité. Dans tous les cas, les personnes les employant au quotidien doivent avoir conscience des risques inhérents à chacune d'elles, et mettre en œuvre les mesures de sécurité nécessaires à leur utilisation. À titre d'exemple, les deux solutions qui suivent peuvent dégrader sensiblement le niveau de sécurité du SI sur lequel elles sont déployées lorsqu'elles sont mal utilisées, mal paramétrées ou encore non mises à jour.

2.1 L'assistance à distance en environnement Microsoft Windows

Les systèmes Microsoft Windows intègrent nativement deux outils de prise en main à distance assez simples d'usage et qui s'appuient tous deux sur le protocole RDP (Remote Desktop Protocol) :

- l'outil de « Connexion Bureau à distance », basé uniquement sur RDP qui lui-même peut s'appuyer sur des mécanismes d'authentification au niveau réseau (Kerberos par exemple) ;
- l'outil d'« Assistance à distance », utilisant entre autres les protocoles MS-RA (Remote Assistance Protocol) et MS-RAI (Remote Assistance Initiator) et ne faisant appel à RDP que pour le déport d'affichage une fois la connexion établie.

À titre d'exemple, l'utilisation de la « Connexion Bureau à distance » standard nécessite l'emploi du compte de l'utilisateur télé-assisté et requiert la connaissance du login et du mot de passe par le télé-assistant. Elle empêche, de fait, de distinguer dans les journaux un accès illégitime à des ressources locales (données, périphériques) et donc, d'identifier toute fuite d'information. Au contraire, une « Assistance à distance », qui serait par exemple à l'initiative de l'utilisateur depuis le centre d'aide et de support, génère un jeton d'accès unique qui est transmis à la personne en charge de la télé-assistance. Par ce biais, l'utilisateur ne communique pas son mot de passe. Il conserve le contrôle des opérations effectuées au travers d'un affichage partagé et, en cas d'incident, l'exploitation ultérieure des journaux d'événements en est facilitée. L'outil d'« Assistance à distance » s'avère donc bien plus adapté à un usage de télé-assistance que ne l'est celui de « Connexion Bureau à Distance », plus adapté à des tâches de télé-administration.

S'agissant du protocole RDP sous-jacent, il a régulièrement évolué depuis sa version 4.0 apparue sous Windows NT Server 4.0, tant au niveau des fonctionnalités que celui de la sécurité. Mis en œuvre aujourd'hui en version 10.2 depuis Windows 10 *Redstone 1*, sa sécurité a évolué au fur et à mesure, souvent pour corriger des vulnérabilités. Il est par conséquent necéssaire d'appliquer les correctifs de sécurité de RDP lors de leur publication, les vulnérabilités correspondantes pouvant affecter les outils « Connexion Bureau à distance » et « Assistance à distance ».

Cette note technique n'ayant pas vocation à détailler les différentes versions du protocole RDP et les vulnérabilités associées, le lecteur souhaitant approfondir ces points est invité à prendre connaissance de la publication scientifique sur la sécurité de RDP exposée au SSTIC 2012 [2]. Les différents avis de sécurité relatifs au protocole RDP peuvent être consultés sur le site du CERT-FR [3], et en particulier

1. Se reporter à la page https://fr.wikipedia.org/wiki/Attaque_de_l'homme_du_milieu.
2. https://www.sstic.org/2012/presentation/securite_rdp/.
3. http://www.cert.ssi.gouv.fr.

les dernières alertes publiées dont celle datant du 12 août 2015 [4] relative à de multiples vulnérabilités dans RDP permettant une exécution de code arbitraire à distance.

2.2 VNC (Virtual Network Computing)

VNC est pour sa part la solution largement utilisée pour la prise en main à distance sur environnements Unix/Linux (mais également quelques fois sous Windows). Cet outil n'intègre quasiment pas de fonctionalités de sécurité, et en l'occurence :

- il repose sur un mécanisme d'authentification faible utilisant un chiffrement symétrique DES dont la clé est dérivée de manière déterministe des 8 premiers caractères du mot de passe ;
- il n'implémente aucun mécanisme de chiffrement des échanges.

Seule la mise en œuvre d'une solution complémentaire établissant préalablement un tunnel chiffré entre le poste télé-assisté et le poste du télé-assistant permet de garantir la confidentialité et l'intégrité des échanges réalisés par VNC. Il est par conséquent fortement déconseillé d'utiliser VNC sans mesures de sécurité complémentaires.

Cette solution ne dispose par ailleurs pas de mécanisme de demande d'assitance. La connexion est à l'intiative du télé-assistant, mais il est toutefois possible de configurer VNC de sorte que l'utilisateur télé-assisté puisse accepter ou rejeter la connexion lorsque la télé-assistance lui est proposée.

Pour en savoir plus sur les vulnérabilités propres à VNC, le lecteur est invité là aussi à prendre connaissance des différents avis de sécurité publiés sur le site du CERT-FR.

3 Recommandations minimales à respecter

Indépendamment de tout contexte et de toute solution de prise en main à distance pour les opérations de télé-assistance, les 12 recommandations suivantes s'appliquent. Lorsque les solutions utilisées le permettent, ces recommandations doivent être imposées techniquement.

R1 - Télé-assistance dans le contexte utilisateur

L'opération de télé-assistance doit s'effectuer dans le contexte de l'utilisateur, avec ses droits, et sans que son mot de passe ne soit communiqué au télé-assistant.

Il est donc important de bien distinguer la télé-assistance de la télé-administration par prise en main à distance. La première s'opère dans le contexte de l'utilisateur, à la différence de la deuxième qui s'opére avec un compte à privilèges dédié à cet usage.

R2 - Supervision des opérations effectuées

La télé-assistance du poste de travail doit s'effectuer de manière visible par affichage partagé entre l'utilisateur et le télé-assistant. L'utilisateur doit être en mesure de voir les opérations effectuées par le télé-assistant.

4. http://www.http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-336/.

L'utilisateur peut ainsi contrôler les opérations réalisées et s'assurer que la confidentialité de ses données n'est pas compromise et que ses droits ne sont pas utilisés à tort.

R3 - Consentement du télé-assisté

L'opération de télé-assistance sur le poste de travail de l'utilisateur doit respecter le consentement de ce dernier. Elle ne doit être possible que suite à l'acceptation explicite de l'utilisateur (dans le cas d'une offre d'assistance) ou à l'initiative de ce dernier (demande d'assistance). Toute connexion arbitraire à un poste de travail utilisateur par un télé-assistant doit être impossible.

R4 - Authentification du télé-assistant

L'authentification des télé-assistants sur les postes distants doit idéalement être réalisée à l'aide de certificats individuels délivrés par une IGC de confiance (ou bien à l'aide de tickets Kerberos délivrés suite à une authentification par certificat individuel par exemple).

Lorsque seul un usage de mots de passe est possible, il convient de prendre en compte le document précisant les recommandations de sécurité sur les mots de passe [5]. Des méthodes d'authentification alternatives par jetons ou mots de passe d'accès uniques peuvent également être suffisantes.

R5 - Limitation des comptes de télé-assistants

L'offre d'assistance, lorsqu'elle est utilisée, ne doit être réalisable que par des télé-assistants dûment autorisés à le faire. Cette restriction pourrait par exemple consister en une liste blanche de groupes ou de comptes utilisateurs autorisés à offrir une télé-assistance.

R6 - Vérification de l'identité du télé-assistant

Dans le cadre d'une offre d'assistance, l'utilisateur télé-assisté doit être en mesure de vérifier l'identité du télé-assistant qui lui est présentée préalablement à toute acceptation. L'identité de ce dernier peut être prouvée par exemple par la présentation d'un certificat X509 ou du compte Active-directory utilisé.

R7 - Lancement de l'application de télé-assistance

La solution de télé-assistance doit se présenter sous la forme d'une application pouvant être démarée par l'utilisateur plutôt qu'un service lancé automatiquement au démarrage du poste de travail.

5. http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf.

R8 - Maintien en condition de sécurité

La solution de télé-assistance doit être à jour de ses correctifs de sécurité en permanence, et mise à jour sans délai dès lors qu'une version plus sécurisée est disponible.

Une vulnérabilité affectant une solution de prise en main à distance peut en effet permettre l'élévation de privilèges rapide par une personne malveillante.

R9 - Postes de télé-assistance

Les postes de télé-assistance doivent être dédiés à ces opérations, isolés d'Internet et en permanence à jour de leurs correctifs de sécurité.

R10 - Fonctions de sécurité portées par la solution

La solution de télé-assistance doit reposer sur des protocoles sécurisés. Les mécanismes de sécurité implémentés doivent permettre :
- une authentification mutuelle entre les postes de télé-assistant et télé-assisté ;
- un échange de clés de session éphémères à la manière de TLS ou d'IPsec ;
- une protection contre le rejeu ou les attaques de type « homme du milieu ».

Pour satisfaire cette recommandation, un tunnel chiffré (IPsec) mis en œuvre préalablement entre les postes à l'aide d'une solution tierce ayant fait l'objet d'une qualification de sécurité par l'ANSSI, a minima d'une certification de sécurité de premier niveau, pourra s'avérer nécessaire.

R11 - Restriction des adresses IP des télé-assistants

La télé-assistance ne doit pouvoir être opérée que depuis des adresses IP sources bien identifiées comme étant celles des postes des télé-assistants.

R12 - Journalisation des opérations

L'ensemble des opérations de télé-assistance effectuées doivent être journalisées, idéalement en les distinguant de toute autre action effectuée sur le poste de travail.

Il doit être au minimum possible de savoir quelle personne s'est connectée à quel poste de travail utilisateur pour une opération de télé-assistance, quand et pendant combien de temps.