Télétravail : échanger en gardant le contrôle de ses données

Charles BLANC ROLIN
RSSI du GHT 15

La situation sans précédent que nous vivons a clairement fait augmenter nos besoins en matière de télétravail et d'échanges numériques. De nombreuses organisations n'étaient pas prêtes, ou pas dans une telle mesure en tout cas. Accès Internet, VPN ou solution de bastion, partage de fichiers, vidéo-conférences, etc... Quelle DSI peut prétendre avoir tout anticipé et permis à l'ensemble des employés de « télétravailler » en toute sécurité ?

Dans le secteur de la santé, nous n'étions, évidemment, pour la plupart, pas préparés à mettre en place une telle organisation de travail à distance pour un aussi grand nombre. À notre « décharge », la majorité des activités, et notamment celles qui composent le cœur de métier de nos établissements, ne peut pas être réalisée à distance. Malgré tout, de nouveaux besoins numériques se sont fait sentir, en particulier les vidéo-conférences, parfois même d'un bout à l'autre de l'établissement, ainsi que les partages « en masse » de fichiers.

Beaucoup ont opté pour les solutions « faciles » proposées par les géants américains du numérique, comme Teams, la solution collaborative de Microsoft qui permet entre autres le partage de fichiers, ainsi que la mise en place de vidéo-conférences, et qui n'a d'ailleurs pas résisté à l'effet Covid-19[1]. L'application de vidéo-conférence Zoom a elle aussi connu la rançon du succès en se faisant décortiquer par les experts en sécurité de la planète. Les résultats ont de quoi faire peur, plusieurs vulnérabilités, un discours commercial pas très franc, un chiffrement très loin d'être digne d'un vieux décodeur Canal + et des données qui transitent par la Chine[2]…

Entre le Cloud Act américain et le niveau de protection des données à caractère personnel chinois reconnu inadéquat par l'Union Européenne, il n'y a pas de quoi se réjouir.

Vous me direz, tout dépend des usages, tant que des informations sensibles ne sont pas échangées, cela ne pose pas vraiment de problèmes.

Dans le cas contraire, quelles solutions utiliser sans perdre le contrôle total de nos données ?

Quitte à investir dans des solutions, pourquoi ne pas se tourner vers des produits français, et cerise sur le gâteau, reconnus par notre Agence Nationale de la Sécurité des Systèmes d'Information ?

Côté partage de fichiers, Oodrive propose des services Saas qualifiés Secnumcloud par l'ANSSI[3], et pour ne rien gâcher, la société est également certifiée Hébergeur de Données de Santé[4], ce qui permet à nos établissements d'y déposer en toute légalité, des données qui concerneraient nos patients.

Sur le plan vidéo-conférence, Tixeo propose une solution disposant d'une certification CSPN, ainsi que

[1] https://www.zdnet.fr/actualites/microsoft-teams-en-panne-en-europe-39900753.htm
[2] https://www.dsih.fr/article/3710/covid-19-et-video-conference-pourquoi-zoom-n-est-pas-la-solution-ideale.html
[3] https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf
[4] https://esante.gouv.fr/labels-certifications/hds/liste-des-herbergeurs-certifies

d'une qualification ANSSI[5]. Elle est disponible en mode Saas, mais également « On Premise ». Elle pourrait donc permettre au-delà des conférences, la réalisation de télé-consultations en hébergement interne ou HDS. C'est à ce jour, une des rares solutions que je connaisse, proposant un véritable chiffrement de bout en bout, et comme la Statue de la Liberté, elle est 100 % française !

Au-delà des solutions commerciales, les solutions libres peuvent également venir à la rescousse !

Jitsi est une excellente solution de vidéo-conférence plébiscitée par Edward Snowden en personne[6] et notamment utilisée par la Direction Interministérielle du Numérique (DINUM)[7]. Elle fait également partie des produits recommandés depuis plus de deux ans déjà dans le SILL (Socle interministériel des logiciels libres)[8], rejointe cette année par la solution BigBlueButton orientée éducation.

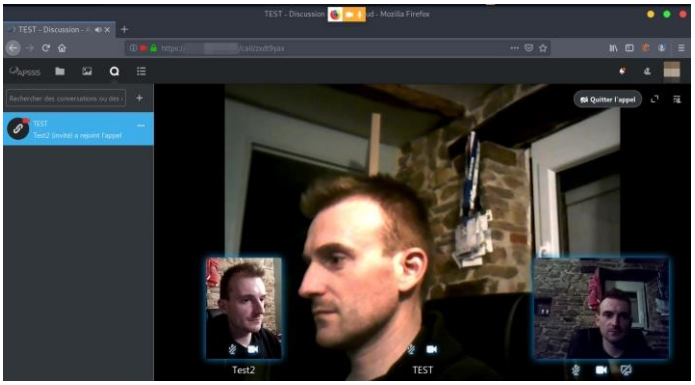
Jitsi ne permet pas encore le chiffrement de bout en bout, même si cela semble être « dans les tuyaux »[9]. En revanche, il permet un chiffrement du flux via le protocole DTLSv1.2, pour lequel il est possible d'utiliser un certificat créé à l'aide d'OpenSSL ou, mieux encore, un certificat renouvelé régulièrement et reconnu par l'autorité Let's Encrypt, à l'aide de l'excellent outil Certbot[10]. Par défaut, le mécanisme d'authentification pour la mise en place d'une réunion, n'est pas activé également, ce qui peut très rapidement poser des problèmes de performances et de bande passante si tout le monde s'invite sur votre serveur. Seul point noir de la solution, la création de comptes utilisateurs et le changement de mot de passe ne peuvent être réalisés que depuis un terminal, en lignes de commandes. Des clients existent pour tous les systèmes d'exploitation, mais comme la solution repose sur le protocole WebRTC, l'utilisation d'un simple navigateur compatible WebRTC, tel que Firefox ou Chromium peut suffire.

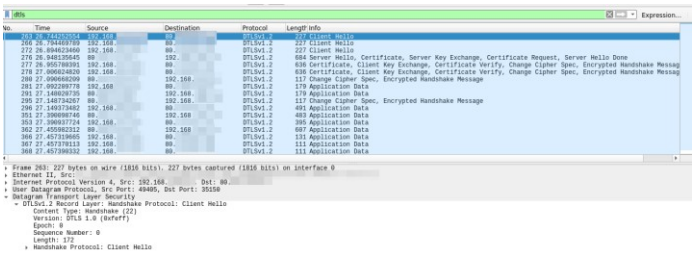
Pour tester la solution ou pour se « dépanner » en cette période de crise, l'hébergeur français Scaleway propose gratuitement des instances Jitsi en libre-service[11].

La solution collaborative Nextcloud qui n'a rien à envier à celles proposées par les GAFAM, après une année en observation dans le SILL 2019[12], fait désormais partie des solutions recommandées[13]. Le Ministère de l'Intérieur a d'ailleurs opté pour cet excellent outil l'an passé[14]. La solution téléchargeable gratuitement (licence AGPL) peut être installée « On Premise » ou pourquoi pas sur une infrastructure HDS. Pour l'avoir essayée, j'ai été réellement bluffé par la solution. Personnalisable à souhait avec plus d'une centaine d'applications disponibles, au-delà du partage de fichiers ou de répertoires d'upload, elle permet notamment la mise en place d'une authentification à deux facteurs (mail, u2f…), chiffrement des fichiers côté serveur, affichage des checksums des fichiers, lecteur de fichiers Keepass, gestionnaire de mot de passe intégré, lecteurs intégrés d'images, de vidéos ou de sons et même lecteur DICOM, permettant de visualiser des images médicales.

[5] https://www.ssi.gouv.fr/qualification/tixeo-server-version-11-5-2-0/
[6] https://www.wired.com/2017/02/reporters-need-edward-snowden/
[7] https://www.numerique.gouv.fr/produits-services/webconference-etat/
[8] https://www.mim-libre.fr/wp-content/uploads/2020/05/sill-2020.pdf
[9] https://jitsi.org/blog/e2ee/
[10] https://certbot.eff.org/
[11] https://ensemble.scaleway.com/
[12] https://www.mim-libre.fr/wp-content/uploads/2019/05/sill-2019-pub.pdf
[13] https://sill.etalab.gouv.fr/fr/software?q=nextcloud&year=2020
[14] https://nextcloud.com/press/pr20190827/

Clou du spectacle, tout comme, Teams, une solution de vidéo-conférence basée sur WebRTC et s'appuyant sur Coturn (STUN/TURN) est aussi intégrée à la solution, avec l'application Talk. Contrairement à Jitsi, le chiffrement de bout en bout est natif[15], et ce, même s'il n'est pas activé dans Coturn qui sert uniquement à la « mise en relation » entre deux terminaux.





Que ce soit avec une solution commerciale ou libre, « télétravailler » de façon souveraine n'est qu'une question de volonté.

[15] https://nextcloud.com/talk/ https://github.com/coturn/coturn/issues/33#issuecomment-467344762