URL :http://www.zdnet.fr/
PAYS :France
TYPE :Web Grand Public

▶ 17 décembre 2020 - 13:19
Cliquez ici pour accéder à la version en ligne

Communications unifiées : Comment maîtriser le phénomène du BYOD

Technologie: La crise sanitaire de la Covid-19 et la généralisation du télétravail ont entraîné une recrudescence du BYOD, mais aussi d'un phénomène honni des DSI, le Shadow IT. Ceux-ci reprennent désormais maintenant la main avec des plateformes UCaaS généralistes. Si l'essor des plateformes de communication unifiée a été vu par les entreprises comme une véritable bouée de sauvetage lorsqu'elles ont dû basculer massivement leur personnel en télétravail, les nouvelles pratiques collaboratives ont parfois favorisé le BYOD et introduit de nouveaux risques.

La crise de la Covid-19 et la généralisation du télétravail a placé les plateformes de communication unifiée au cœur de la survie des entreprises. Elle fut dans de nombreux cas un accélérateur du déploiement à grande échelle de plateformes de type UCaaS. Les plateformes collaboratives sont réellement devenues critiques pour l'activité des entreprises et les DSI y ont vu l'occasion de remettre de l'ordre dans les pratiques collaboratives des utilisateurs métiers qui, faute de solutions adaptées, s'étaient tournés vers des solutions collaboratives disponibles sur internet, depuis Slack, Trello, en passant par WhatsApp, etc. Une approche Shadow IT généralement peu appréciée des DSI.

La récente acquisition de Slack par Salesforce, pour la bagatelle de 27,7 milliards de dollars, démontre l'importance prise par l'approche plateforme dans la collaboration d'entreprise.

Les DSI plébiscitent les grandes plateformes collaboratives

Bien souvent, les DSI ont décidé de remplacer ces multiples solutions par des plateformes plus généralistes, à l'image de Microsoft 365, Google Workspace et quelques autres, dont le français Talkspirit. « En 2020, la grande tendance a été le retour des plateformes », explique Philippe Pinault, CEO de Talkspirit, éditeur français d'une plateforme collaborative. « Entre 2010 et 2020, nous avions vu l'arrivée d'un très grand nombre d'applications dans les entreprises, bien souvent des applications gratuites qui passaient sous le radar. Ces outils étaient très performants et répondaient bien aux besoins opérationnels des équipes métiers. Ces applications et services constituent aujourd'hui une galaxie de solutions sur lesquelles les entreprises ont bien du mal à identifier quelles sont les données qui sont partagées et stockées, sur des services qui sont bien souvent américains. »

L'éditeur français a ainsi largement étendu la couverture fonctionnelle de sa solution collaborative en ajoutant des briques visio, un stockage de type "drive", une solution bureautique basée sur Open Office et bien évidemment le chat, un outil qui s'est puissamment développé dans les entreprises en 2020.

Philippe Pinault, CEO de Talkspirit / Holaspirit :

« La nature ayant horreur du vide, les utilisateurs s'étaient tournés vers des solutions disponibles sur le web et que leur entreprise ne leur fournissait pas. Désormais, les plateformes sont matures, les DSI peuvent siffler la fin de la récréation et imposer une plateforme qui permettra de rationaliser les usages collaboratifs à l'échelle de l'entreprise. »

Les éditeurs de plateformes UCaaS ((Unified Communications as a Service) ont couru derrière les pure player pour intégrer leurs innovations dans leurs plateformes et offrir, si ce n'est 100 % de leurs capacités, celles qui sont les plus fréquemment utilisées en entreprise. « Nous n'avons pas vocation à être aussi complets que les applications spécialisées qui se sont multipliées ces dernières années, c'est évidemment impossible en tant qu'éditeur. Par contre, nous implémentons les 30 % de fonctions qui constituent l'essentiel des usages réels des utilisateurs », résume Philippe Pinault.

Les plateformes UCaaS ont simplifié le passage au télétravail

Autre aspect de ce changement profond des conditions de travail, les plateformes téléphoniques intégrées aux plateformes collaboratives ont permis de traiter les appels entrants des entreprises, sans impact pour les clients. D'autre part, les softphones proposés par certains opérateurs rivalisent avec les meilleurs applications de messagerie grand public, comme l'explique Anthony Lesueur, chef de projet marketing chez Linkt, opérateur télécom partenaire d'intégrateurs Microsoft : « notre softphone offre aujourd'hui de la messagerie instantanée et

des outils de collaboration qui sont bien intégrés aux habitudes des collaborateurs qui utilisent quotidiennement WhatsApp, Facetime ou Messenger sur leurs smartphones personnels. Avec mon softphone Linkt, en quelques secondes je peux échanger et discuter avec mes collègues dans le métro, au bureau ou en rendez-vous ».

Anthony Lesueur, chef de projet marketing chez Linkt :

« Fournir aux collaborateurs une plateforme de communication unifiée est un bon moyen pour les DSI de contenir le phénomène du Shadow IT. En parallèle, les DSI français ont cherché à limiter au maximum le phénomène BYOD en déployant d'énormes efforts pour équiper leurs collaborateurs, épuisant les stocks de PC mobiles et de casques audio chez tous les distributeurs. »

Le passage d'une téléphonie d'entreprise classique, basée sur un PABX ou un IPBX, à une plateforme UCaaS, a simplifié le passage au télétravail. Certains collaborateurs ont pu utiliser le softphone préconisé par leur entreprise sur leur smartphone personnel, lorsqu'ils ne disposaient pas d'un PC portable ou d'un smartphone d'entreprise.

Tolérance envers le BYOD

Néanmoins, dès l'annonce du premier confinement, les DSI ont pillé les stocks de PC portables et casques audio chez les distributeurs, pour équiper un maximum de collaborateurs. Car si pendant les premiers jours certains ont fait preuve de plus de tolérance qu'à l'accoutumée vis-à-vis du BYOD, ceux-ci ont rapidement repris les rênes de leur système d'information.

Contrairement aux idées reçues, pour l'expert, le véritable risque n'a pas réellement porté sur le risque d'infection par des malwares. Les PC domestiques sont infectés par des malwares relativement classiques que les antivirus ou EDR peuvent détecter relativement facilement et bloquer avant qu'ils n'infectent les serveurs de l'entreprise. Néanmoins c'est au niveau de la fuite de documents que l'usage du BYOD pose problème. Les collaborateurs sont potentiellement tentés de stocker sur leur poste des documents confidentiels hors de tout contrôle de leur entreprise. De plus, une attaque sur ses postes à la sécurité non maîtrisée peut permettre à un hacker de mettre la main sur les identifiants de l'utilisateur et s'introduire dans le SI de l'entreprise.

Jean-Michel Tavernier, directeur France de MobileIron :

« Au début du confinement, beaucoup de PME n'avaient pas assez d'ordinateurs portables à distribuer à leurs collaborateurs. Beaucoup de services comme les RH, l'approvisionnement et autres n'avaient pas pour habitude de travailler à distance. Les collaborateurs ont donc installé leur messagerie sur leurs tablettes, leur PC familial, ce qui leur a permis de travailler dès le début du confinement, mais ce qui a aussi ouvert de grandes failles de sécurité. »

Les DSI ont repris le contrôle

Après un déploiement en mode éclair lors des premiers jours du confinement, les DSI ont "resserré les boulons". Certaines PME ont mis en place une plateforme de MDM (Mobile Device Management), afin de gérer à distance l'ensemble des postes clients amenés à se connecter à leur système d'information, avec la possibilité d'imposer des connexions via des terminaux appartenant à l'entreprise et tolérer des smartphones personnels mais via un espace professionnel protégé dans un conteneur spécifique. « Une plateforme MDM permet notamment de vérifier le numéro de version de l'OS et les niveaux de patchs installés ainsi que les mises à jour des applications, ce qui permet déjà de résoudre bon nombre de failles de sécurité », ajoute Jean-Michel Tavernier.

Autre chantier en cours pour améliorer la sécurité de ces systèmes d'information, qui doivent assumer le télétravail généralisé sur une longue durée, le "Zero Trust". L'informatique va s'assurer à tout moment que toute demande de connexion reste cohérente avec le profil de chacun : un utilisateur qui se connecte habituellement en région PACA depuis un iPhone et qui le même jour tente de se connecter à nouveau depuis un smartphone Android en Asie va déclencher l'alerte. De même, le "Single Sign-On", une fonctionnalité bien utile pour se connecter à de multiples applications sans avoir à saisir continuellement ses mots de passe, est aussi un moyen d'éviter la fuite de mots de passe.

Les DSI doivent déployer les solutions qui vont permettre de pérenniser la sécurité de leur système d'information, alors que le télétravail à grande échelle semble amené à perdurer.