QUODAGIS
Managed Services

Bonnes Pratiques
en matière de support distant

QUODAGIS
Managed Services

La plupart des supports distants ou externalisés utilisent aujourd'hui des outils de contrôle à distance pour fournir le service d'assistance aux utilisateurs.
Ce document tente d'apporter des réponses à tout ce que vous avez voulu savoir sur le support à distance et que vous n'avez jamais osé demander…

> Pourquoi utiliser un support à distance ?
> Comment peut-il être efficace ?
> Qui dans mon organisation fournit une assistance à distance ?
> Comment sont appréhendés les sujets de confidentialité ou de vie privée ?
> Quelles sont, le cas échéant, les bonnes pratiques dans ce domaine ?

De toute évidence, les outils de contrôle à distance («shadowing») sont devenus l'un des éléments clés de la technologie de support avec l'ITSM. Avec un nombre croissant de sollicitations, et la recherche permanente de contrôle des coûts de support, un logiciel de prise en main à distance permet de réduire significativement (parfois même de supprimer) le temps nécessaire d'intervention de proximité sans dégrader l'expérience utilisateur.

Souvent, l'équipement d'un client, ordinateur, tablette ou smartphone, peut être rapidement remis en fonction par l'addition d'un patch ou une mise à jour, un changement de configuration ou un ajustement des paramètres. Mais les utilisateurs n'ont pas toujours les droits et autorisations nécessaire pour effectuer ces changements, ne savent pas où obtenir le logiciel nécessaire, ou ne sont même pas conscients qu'ils aient besoin d'un logiciel ou d'ajustements de paramètres.

Par ailleurs, certaines estimations disent que les travailleurs mobiles ou itinérants constitueront la majeure partie de la main-d'œuvre très rapidement. Ces utilisateurs finaux auront besoin d'une assistance rendue possible à distance par les outils de contrôle et de prise en mains.
Travailler à distance impose d'être en mesure de partager un écran et effectuer des opérations sur un équipement distant.

LES BÉNÉFICES DU SUPPORT DISTANT

Confier à un personnel compétent la charge d'assistance et de soutien à ses utilisateurs tout en leur permettant d'utiliser une technologie de support à distance apporte un certain nombre de bénéfices :

> Facilite la collecte d'informations nécessaire au diagnostic,
> Meilleure analyse des causes et des impacts,
> Résolution au premier contact,
> Gain du temps dans la résolution,
> (in)Formation des utilisateur aux méthodes de diagnostic et de résolution en vue de l'auto-résolution des futurs incidents
> Satisfaction au travers d'un bonne expérience utilisateur et Fidélisation des clients (User ExperienceDesign),
> Capacité à gérer un volume important de ticket sous pression.

SÉCURITE ET CONFIDENTIALITÉ

Avoir accès aux ordinateurs des autres, que ce soit au sein de l'organisation ou à l'extérieur de celle-ci, pose pour le centre de support à la fois des questions en termes de conformité et d'éthique. Chacun doit avoir pleinement conscience de ces considérations, qu'il soit utilisateur, client ou fournisseur. Et ces considérations doivent être connues et partagées.

Prenons, par exemple, un contrôleur de gestion ou un autre membre de l'équipe des finances qui rencontre de sérieux problèmes avec son tableur. Afin de résoudre le problème, un technicien de support aura probablement besoin de se connecter à distance à l'ordinateur du contrôleur de gestion alors que le classeur de données en cause est ouvert. Le classeur peut très bien contenir des données confidentielles ou sensibles. La même chose peut être dite pour la connexion à des ordinateurs de la DRH, du service juridique, de la Direction même, et de nombreux autres départements ou des groupes au sein d'une entreprise. De même, les établissements d'enseignement peuvent s'interroger avant de donner accès à des ordinateurs contenant des questions d'examen, les admissions, et d'autres données sensibles ; la même chose est vraie pour les hôpitaux, les cabinets d'avocats, les cabinets fiscaux, cabinet d'audit ou de courtage, et ainsi de suite … les exemples sont nombreux.

Il faut donc aborder le sujet de la confidentialité de l'information selon les 3 axes suivants :

1. La technologie

Les logiciels permettant de se connecter ou prendre le contrôle à distance varient. Certaines solutions peuvent être utilisées aussi pour le travail collaboratif et le partage d'écran, et ne sont pas exclusivement dédiées au support.

> **Client/server :** Dans ce modèle, le logiciel s'exécute sur le poste du technicien (ou du serveur) et peut se connecter à une application cliente installée sur le poste de l'utilisateur, permettant à un profil administrateur d'avoir une vue complète et le contrôle du poste. Dans certains cas, le logiciel peut être « poussé » par l'administrateur s'il n'a pas été installé préalablement.

> **En ligne (web access) :** Le client ouvre une page web et partage son écran avec un technicien qui récupère (pick-up) la connexion autorisée par le client.

> **Appliance :** Basé sur le matériel, le contrôle des sessions est centralisé.

Quel que soit le type de votre organisation, la sécurité doit être une priorité élevée. Une connexion de support à distance non sécurisée est un risque de piratage et de prise en main de vos équipements par un tiers mal intentionné. Le protocole utilisé pour la connexion doit être sécurisé, et doit se conformer à des exigences telles que PCI DSS, HIPAA, SOX, ainsi que toute autre exigence spécifique à l'industrie ou aux banques. Toutes les connexions à distance doivent être enregistrées automatiquement de sorte que les vérifications puissent être effectuées.

2. Les processus

Il est impératif de définir une procédure standard pour la connexion à un ordinateur pour une opération de support à distance. De nombreux produits de contrôle à distance ont une fonction qui avertit l'utilisateur quand une connexion est faite, et peut exiger l'autorisation préalable de cet utilisateur.

De la même façon, l'utilisateur est prévenu que la connexion est terminée et l'accès désactivé. Lorsque cette fonction existe, elle doit être activée pour que les clients / utilisateurs finaux puissent toujours savoir quand les connexions sont faites. Cela permet à l'utilisateur, selon son contexte, de retarder ou de refuser l'intervention à distance. Si votre organisation utilise un produit de contrôle à distance qui ne propose pas cette fonctionnalité, il est fortement conseillé de mettre en place un processus de demande d'autorisation et d'information écrit (un email suffit) ou verbale (téléphone) afin que l'autorisation soit toujours obtenue au préalable de chaque intervention pour une connexion spécifique. En d'autres termes, ce n'est pas parce que vous avez donné votre permission de se connecter à votre ordinateur aujourd'hui que cela signifie que vous l'avez donné pour toujours.
S'il y a besoin de se connecter à nouveau, une nouvelle demande doit être formulée.

3. Les personnes

Au minimum, chaque technicien doit recevoir une formation sur l'importance de suivre des procédures lors de l'utilisation des outils de contrôle à distance – comme pour toute procédure d'ailleurs - , et devrait être invité à signer un code d'éthique ou une charte informatique attestant de son accord pour agir d'une manière honnête, intègre et professionnelle. Il doit y avoir des conséquences appropriées (jusqu'à et y compris la résiliation du contrat de support et les sanctions disciplinaires) pour avoir violé la règle et/ou de ne pas suivre la procédure appropriée.
Toute personne intervenant avec un outil de prise de contrôle à distance dans une organisation doit être consciente qu'elle détient « les clés du royaume ». Elle doit comprendre l'importance de ne pas trahir cette confiance.

Comme pour toute règle, il y a des exceptions, mais elles sont rares. Supposons, par exemple, qu'un poste de travail soit infecté par un virus ou un logiciel malveillant qui tente de se propager à travers tout votre Le réseau. Si, malgré des tentatives vaines et répétées pour alerter l'utilisateur, la meilleure solution et à savoir, la plus rapide, est d'éteindre la machine à distance jusqu'à ce qu'un technicien puisse régler le problème, cette possibilité doit être offerte au technicien. Mais dans ces situations d'urgence, un superviseur ou le gestionnaire doit être consulté pour prendre la décision d'accéder à l'ordinateur et lancer la commande sans l'accord de l'utilisateur. Le technicien ne doit pas prendre de décision unilatérale, et les étapes menant à la décision d'accéder à l'ordinateur distant sans autorisation doivent être documentées. Des cas comme celui-ci doivent être examinés pour voir s'il existe une autre solution, et si les procédures existantes ou les caractéristiques des produits de « commandes à distance » doivent être remplacées ou modifiées.

GÉRER UN VOLUME IMPORTANT DE TICKET SOUS PRESSION

Le fort accent donné au business, couplé avec l'évolution rapide des technologies, génèrent une forte pression sur les équipes de support technique en termes de performance (productivité, efficacité et efficience), et imposent souvent la nécessité de démontrer leur valeur à l'entreprise. Lorsque vous demandez à votre équipe support si elle ressent la pression de prouver sa valeur, la réponse est toujours affirmative. En leur donnant la possibilité de prendre le contrôle d'un équipement informatique à distance et résoudre les incidents, on donne aux techniciens la possibilité de résoudre rapidement les problèmes sans besoin de se rendre physiquement sur le poste.

En fait, les équipes peuvent être mises en place facilement pour fournir une qualité de service élevée - partout dans le monde. Les outils de contrôle à distance sont devenus la technologie la plus évidente pour fournir un support de qualité.

Le nombre d'organisations qui résout plus de la moitié de leurs tickets d'incident à distance est en constante augmentation. Les outils de contrôle à distance et la résolution des incidents sans escalade au second niveau améliorent l'expérience client dans les centres de support.

En plus d'améliorer l'expérience client, cela génère des économies mesurables (Baisse du TCO – Total Cost of Ownership – Coût Global de Possession).

POUR UNE ASSISTANCE SUPPORT À DISTANCE SÛRE ET RÉUSSIE

La mise en œuvre des outils de contrôle à distance, une fois appropriés et sécurisés dans votre organisation, ne doit pas faire oublier l'importance de la formation et de la sensibilisation. Assurez - vous de la compréhension des utilisateurs finaux ou client que le contrôle à distance est une option, qu'ils ont toujours le choix concernant le quand et comment il est utilisé, et que chaque technicien support comprenne les procédures appropriées pour le contrôle à distance.

Il y a de nombreux avantages à l'assistance à distance, elle permet en particulier de montrer aux clients et utilisateurs finaux comment faire quelque chose, et vice versa. Chaque connexion à distance est une occasion de partager de l'information, et il peut fonctionner dans les deux sens. Même le plus honnête des utilisateurs finaux craint d'être "espionné" et peut résister à l'idée d'un contrôle à distance. Soyez clair sur la avantages pour eux et assurez - vous qu'ils comprennent leur niveau de contrôle.

LE CENTRE DE SUPPORT TECHNIQUE DU FUTUR

La capacité des équipes de support informatique pour fournir un niveau exceptionnel de service à la clientèle passera par leur capacité à aider les organisations et leurs employés à comprendre comment tirer parti de façon appropriée des technologies connues et émergentes dans l'entreprise. Les équipes de support informatique devront contribuer à aider les organisations à trouver de nouvelles façons d'utiliser la technologie pour rationaliser les opérations, réduire les coûts et de mieux répondre aux besoins des utilisateurs finaux.

Mais ce sujet mérite à lui seul une autre publication...