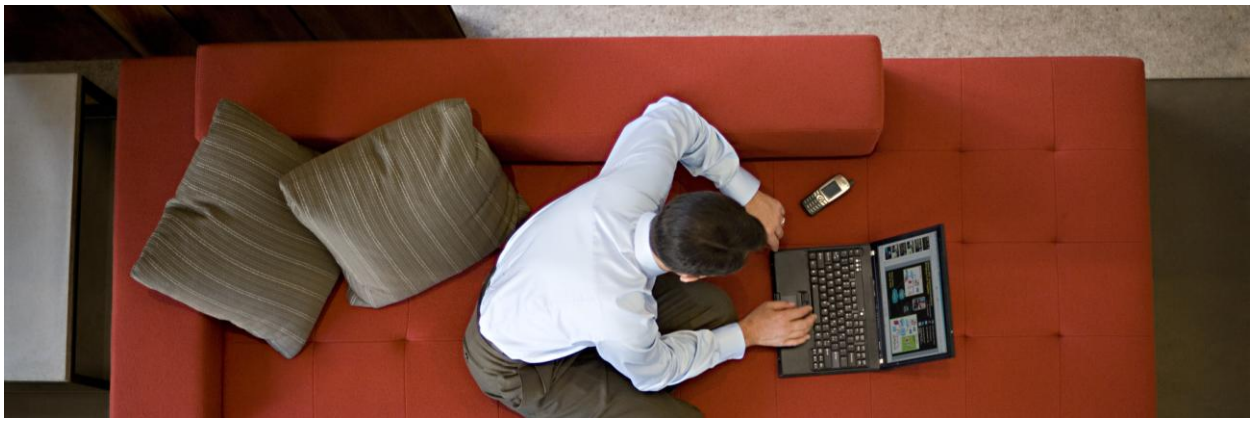


Pandémie : comment assurer la continuité d'activité de l'entreprise ?

Les entreprises françaises sont peu préparées à affronter une éventuelle pandémie

Le concept de plan de continuité d'activité n'est pas nouveau pour les entreprises. Que ce soit pour faire face à une panne d'un équipement ou une indisponibilité du réseau électrique, elles ont le plus souvent mis en place des plans de secours pour pouvoir s'assurer de limiter l'impact de ces événements sur leurs opérations. Ainsi, une étude de Gartner (Gartner EXP) nous apprend que 88% des entreprises se sentent prêtes à affronter une coupure de courant, et 70% la perte d'un serveur ou d'une application. Dans ces cas de figures, la réponse est généralement principalement technologique : onduleurs, redondance des équipements et des liens, sauvegardes, etc.

Toutefois, il reste un type de perturbations que les entreprises ont encore beaucoup de mal à anticiper : celles qui empêchent les employés de se rendre physiquement sur leur lieu de travail. En effet, la même étude nous apprend que seulement 13% des entreprises sont prêtes à y faire face. Certes, ce type de perturbation étant plutôt lié à des événements extraordinaires (sinistres) ou relativement limités dans le temps et/ou l'espace (grèves des transports, intempéries), ces statistiques peuvent sembler assez peu inquiétantes en temps normal. Cependant, les craintes d'une apparition d'une pandémie de grippe A nous incitent à nous pencher sur ce problème avec un œil nouveau. Que se passera-t-il si, pour éviter une trop grande propagation de la maladie, les entreprises sont amenées à renvoyer l'ensemble de leurs employés chez eux ? Combien seront capables de poursuivre normalement leurs activités dans un tel contexte ? Vraisemblablement assez peu. Quel sera le niveau d'impact sur leur productivité et leur rentabilité ? Probablement très élevé.

Et pourtant il existe là aussi des réponses technologiques qui, intégrées dans une stratégie de gestion des risques décidée en amont, permettent de gérer cette situation. Il s'agit bien entendu des outils de télétravail et, de manière plus large, de l'ensemble des solutions permettant de travailler et de collaborer à distance que nous allons détailler par la suite.

Au préalable, il convient toutefois de noter que si peu d'entreprises sont prêtes à affronter ce type de difficultés, c'est avant tout parce que les principaux freins à l'adoption du télétravail ne sont le plus souvent pas technologiques mais plutôt culturels. Il reste encore bien souvent du côté des employeurs des réticences liées principalement à une certaine suspicion vis-à-vis des employés qui pratiquent le télétravail : on préfère encore bien souvent les avoir « sous la main ». Et, du côté des employés, les freins culturels existent également. Ainsi, une étude de 2007 plaçait

les salariés français au 25ème rang européen (sur les 27 pays de l'UE) pour ce qui est de l'intérêt pour le télétravail, loin derrière les pays nordiques notamment. Au total, comme le soulignait le plan gouvernemental France Numérique 2012, on constate que le télétravail concerne en France uniquement 7 % de la population active, contre en moyenne 13 % en Europe et 25 % aux États-Unis. Les entreprises françaises profitent donc moins que les autres des avantages du télétravail, que ce soit en termes de performance et de productivité mais aussi d'éco-responsabilité (moins de transports donc réduction de l'empreinte carbone) ou de qualité de vie des employés, sujets qui deviennent également de plus en plus d'actualité. Alors, peut-être que la pandémie de grippe A, si elle a lieu, va les obliger à avancer à marche forcée mais, indépendamment de tels événements dont on ne peut bien entendu qu'espérer qu'ils ne se produisent pas, il est important qu'elles s'interrogent dès aujourd'hui sur les évolutions culturelles et organisationnelles à mettre en œuvre pour tirer parti des pratiques de télétravail.

Préparer son plan de continuité

Intéressons-nous à présent aux solutions qui vont permettre d'organiser le travail de façon à ce que l'activité de l'entreprise soit maintenue que les employés aient la possibilité ou non de se rendre physiquement sur leur lieu de travail. Comme pour tout déploiement technologique, il convient avant de se lancer tête baissée de mener une réflexion approfondie pour bâtir la solution la mieux adaptée au contexte de l'entreprise.

La première étape est bien entendu l'évaluation des risques. Il va s'agir de répondre à quelques questions telles que :

- Quels seraient les impacts si un sinistre ou une pandémie devaient bloquer l'activité un jour, une semaine, voire plusieurs mois ?
- Quelles sont les services ou départements les plus critiques dont l'activité doit impérativement être maintenue en priorité ?

Ensuite, il convient de déterminer quelles règles et pratiques il faudra mettre en œuvre. Il va ici falloir :

- Catégoriser les rôles et la responsabilité des employés : quels employés doivent accéder à quelles applications ou informations ?
- Organiser des groupes d'employés en fonction de leurs besoins de communication

Ensuite, il est bien entendu nécessaire de mener un audit des solutions déjà en place et de définir quelles nouvelles solutions il va falloir mettre en œuvre :

- Recenser les équipements disponibles (combien d'ordinateurs portables à disposition ?)
- Analyser les solutions d'accès distant existantes et leur capacité à monter en charge (une solution utilisée par 50 utilisateurs aujourd'hui va-t-elle être à même de supporter 1000 utilisateurs simultanés si le besoin s'en fait sentir ?)
- Auditer les capacités du réseau et identifier les manques
- Préparer un plan de déploiement et de test des nouvelles solutions

Enfin, on l'a vu, la dimension culturelle du télétravail est extrêmement importante et il est primordial de préparer également un plan de communication qui va permettre d'expliquer aux employés les raisons de la mise en place des solutions et de les former à leur utilisation.

Quelles solutions dans le cas d'une pandémie ?

Dans le cas spécifique de la pandémie, les objectifs de la solution à mettre en œuvre sont multiples :

- Permettre aux employés d'effectuer leur mission depuis chez eux ou depuis n'importe quel autre lieu en accédant aux outils et informations dont ils ont besoin exactement comme s'ils étaient au bureau
- Fournir une flexibilité maximum en termes d'environnement de télétravail : ordinateur appartenant à l'entreprise ou à l'employé, terminaux mobiles, accès depuis des bornes internet publiques, etc.
- Etre capable de supporter un pic d'activité : contrairement à une solution d'accès distant en temps normal, il va falloir supporter la connexion simultanée de quasiment tous les employés.
- Assurer une sécurité totale et personnaliser les niveaux d'accès en fonction de l'utilisateur, du terminal ou du lieu depuis lequel s'effectue la connexion
- Minimiser les équipements supplémentaires nécessaires au domicile de l'employé
- Faciliter et fluidifier le provisionning et l'administration de la solution en minimisant le besoin d'intervention de la part du télétravailleur

Pour atteindre ces objectif, on va alors faire appel à un ensemble de technologies diverses et variées : réseau privé virtuel (ou VPN – Virtual Private Network), téléphonie sur IP, conférences et outils collaboratifs. Ces technologies vont être combinées pour apporter un niveau de réponse adapté aux besoins définis pour chaque utilisateur (en fonction de son rôle, de son équipement, etc.), tout en maintenant la sécurité des données critiques de l'organisation. Ainsi, Cisco propose quatre niveaux de solutions, en fonction de la fréquence et du niveau d'accès nécessaire d'une part, de l'investissement financier d'autre part :

- Réunions virtuelles et partage de document
- Accès aux données simple et universel via un navigateur web
- Extension du réseau wifi/téléphonique au domicile de l'utilisateur
- Extension complète du bureau à la maison

Réunions virtuelles et partage de document

Le premier niveau de réponse est l'utilisation d'une solution de collaboration en ligne qui va permettre d'organiser des conférences audio et de partager des documents (une présentation powerpoint par exemple). Ainsi, les employés peuvent continuer à tenir leurs réunions ensemble ou avec leurs clients et partenaires sans avoir besoin de se rencontrer physiquement.

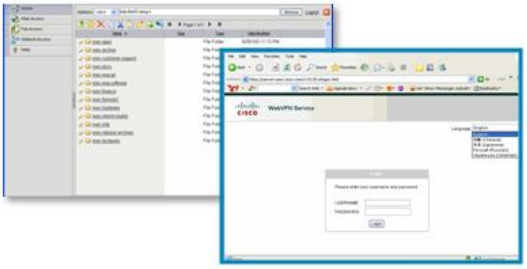
Dans ce domaine, Cisco propose sa solution Webex qui apporte en plus des services avancés tels que le multimédia (vidéo), l'enregistrement des sessions ou le chat.

En outre, comme cette solution repose sur l'infrastructure Cisco Collaboration Cloud, l'entreprise n'a aucun équipement supplémentaire à installer et elle a l'assurance que le service pourra suivre l'évolution du besoin, quel que soit le nombre d'utilisateurs requis. Il suffit pour l'employé de disposer d'un ordinateur (personnel ou professionnel) connecté à internet pour pouvoir commencer à l'utiliser. Peu importe le terminal ou le système d'exploitation utilisé, le simple téléchargement d'un plug-in lors de la première utilisation permet de profiter du service. Enfin, proposé sous forme d'un service mensuel (à l'usage), Webex apporte également une grande souplesse en termes de tarification.

Accès aux données simple et universel via un navigateur web

Le deuxième niveau de réponse est d'offrir aux employés un accès aux données, applications et informations qui sont stockées au sein même du système d'information de l'entreprise. Il va donc s'agir de mettre en place un accès distant sécurisé au réseau et on fait appel pour cela à la technologie du réseau privé virtuel (VPN) qui consiste à utiliser internet pour permettre à un utilisateur distant de se connecter sur le réseau de l'entreprise via un « tunnel » sécurisé. On distingue VPN IPSec et VPN SSL.

Le VPN IPSec présente l'avantage de permettre à l'employé d'accéder intégralement au système d'information et de retrouver complètement son environnement de travail habituel mais nécessite l'installation d'un logiciel (un client VPN) sur le poste de l'utilisateur.



A l'inverse, le VPN SSL ne nécessite pas d'installation de client. L'utilisateur se connecte depuis un navigateur à un portail web paramétrable en fonction de son profil, en utilisant un identifiant et un mot de passe. Il peut le faire depuis n'importe quel type d'ordinateur (professionnel, personnel ou même PC en libre-service) et peut ainsi accéder à des fichiers en mode web et à un certain nombre d'applications.

Si, une fois installé, le VPN IPSec peut généralement apporter un plus grand confort et une plus grande richesse d'utilisation, on comprend bien que dans le cas d'une pandémie, sa relative complexité de mise en œuvre le rend moins adapté que le VPN SSL. En effet, dans ce cas précis, il est compliqué d'organiser le déploiement du client VPN alors que tous les utilisateurs ne disposent pas nécessairement d'un ordinateur portable fourni par l'entreprise et que certains vont probablement être amenés à se connecter via un ordinateur personnel.

La difficulté qui se présente alors est la sécurité. En effet, comment s'assurer que des utilisateurs qui se connectent avec des ordinateurs dont on ne maîtrise pas le contenu ne vont pas venir infecter le réseau de l'entreprise ? Il existe la aussi une réponse technologique : lorsque l'utilisateur se connecte en VPN SSL on créé une sorte de « bureau virtuel » qui isole totalement la session VPN du reste de l'ordinateur.

Dans tous les cas, la mise en œuvre d'accès VPN implique l'installation d'un équipement spécifique sur le réseau de l'entreprise. Cisco propose plusieurs types de solutions, la principale étant le boîtier de sécurité Cisco ASA qui intègre un pare-feu, la gestion VPN, le filtrage de contenu et une solution anti-X, et offre un mode de licence particulièrement adapté aux conditions de pandémie. En effet, il est possible d'augmenter à coût réduit le nombre d'utilisateurs sur une courte période (2 mois maximum) pour répondre à un pic d'activité, alors que les déploiements VPN sont généralement dimensionnés pour pouvoir supporter la connexion simultanée d'environ 10% des utilisateurs, ce qui risque probablement d'être insuffisant dans le cas d'un événement de ce type.

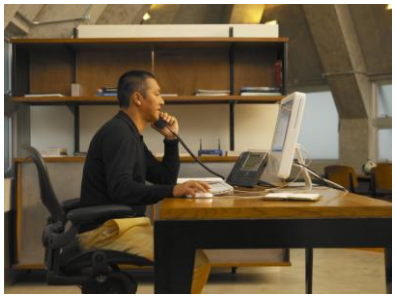
Extension du réseau wifi/téléphonique au domicile de l'utilisateur

Le troisième niveau de réponse est un niveau de service et une souplesse supplémentaires apportés aux entreprises déjà clientes Cisco. Il s'applique à des employés qui vont accéder au réseau depuis leur domicile (plutôt qu'en situation de nomadisme depuis tout type de lieu) et vraisemblablement plutôt de manière régulière, au-delà du simple contexte d'une pandémie. Il peut prendre deux formes :

Pour les entreprises qui disposent déjà d'un réseau wifi Cisco, il s'agit de créer une extension du réseau wifi de l'entreprise au domicile de l'employé en ajoutant simplement une borne wifi derrière l'équipement d'accès installé par son fournisseur d'accès internet. La sécurité va bien entendu être totalement assurée entre la borne et le réseau de l'entreprise et l'employé va ainsi pouvoir travailler depuis son domicile exactement comme s'il était assis à un bureau dans les locaux de l'entreprise en profitant de tous les services auxquels ils est habitués : messagerie, applications métiers, serveurs de fichiers, etc.

De la même manière, pour les entreprises équipées d'un système de téléphonie sur IP Cisco et d'un boîtier ASA, il est possible de simplement ajouter un téléphone IP derrière l'équipement d'accès à internet au domicile de l'employé pour qu'il puisse retrouver son environnement téléphonique (numéro de ligne, raccourci, messagerie vocale…) exactement comme s'il était au bureau. Une solution particulièrement intéressante pour des entreprises dont l'essentiel de l'activité se fait par téléphone.

Extension complète du bureau à la maison



Le quatrième et dernier niveau de réponse s'adresse lui aussi plutôt à des télétravailleurs très réguliers et consiste à re-créer entièrement l'environnement de travail du collaborateur à son domicile pour lui apporter une expérience strictement identique à celle des employés basés dans les locaux de l'entreprise. Il faut pour cela installer un routeur et un téléphone IP à son domicile. Cette solution permet en outre de créer un accès internet séparé pour la famille afin qu'il soit possible de continuer à utiliser internet à titre personnel sans que cela ne perturbe l'activité de l'entreprise. Enfin, elle apporte également une grande souplesse dans l'administration puisque les équipes informatiques sont incapables d'intervenir facilement à distance sur les configurations de l'ensemble des routeurs du parc.

On le voit, même dans un cas aussi extrême que celui d'une pandémie, il existe bel et bien des solutions pour permettre aux entreprises de poursuivre leurs activités en apportant un niveau de service adapté aux besoins spécifiques de chacun de leurs employés. Il n'en reste pas moins que les entreprises françaises se les sont peu appropriées à ce jour et on ne peut donc que les encourager à s'y intéresser afin de se préparer à parer à toute éventualité.

Pour en savoir plus

Cisco Webex

www.webex.fr

Cisco ASA

www.cisco.fr/go/asa

www.cisco.com/go/asa (en anglais)

Toutes les solutions Cisco pour le télétravail

http://www.cisco.com/en/US/netsol/ns340/ns394/ns430/index.html (en anglais)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.