# Marco Rottigni, Qualys : «La priorité est désormais d'accompagner le télétravail et d'assurer la sécurité du parc»

**La crise sanitaire a-t-elle remis à plat les plans stratégiques des DSI ?**
**Marco Rottigni –** Lorsqu'ils ont préparé leur stratégie pour 2020, de nombreux services informatiques ont établi des plans généraux sur la transformation numérique et sur la façon dont le Cloud et les logiciels allaient pouvoir soutenir cet objectif.
Aujourd'hui avec la crise Covid-19 ce n'est plus une option, il faut gérer le télétravail et les opérations à distance. La priorité est désormais d'accompagner le télétravail et de veiller à ce que tout se passe pour le mieux, notamment parvenir à assurer la mise à jour et la sécurité du parc informatique à un moment où l'équipe IT n'exerce qu'un contrôle réduit et sans accès physique aux équipements concernés.

**Concrètement, qu'est qui va changer ?**
**Marco Rottigni –** Les collaborateurs qui travaillent à distance utilisent soit leurs équipements personnels, soit des systèmes fournis par leur employeur. Si la fourniture des équipements et de l'accès à Internet ne pose pas de réel problème, la gestion de l'aspect sécurité s'avère plus délicate. En préalable à tout télétravail, le service informatique doit veiller à appliquer les correctifs et les mises à jour sur les équipements et à déployer des logiciels de sécurité traditionnels tels que des firewalls et des applications antivirus.

Cependant, l'apparition du coronavirus provoque deux changements de taille. D'une part, dans l'immédiat, ces actifs ne sont pas connectés au réseau de l'entreprise. Autrement dit, les ordinateurs portables et autres actifs ne sont plus protégés par le firewall de l'entreprise ou par d'autres technologies de sécurité périmétrique déployées de manière centralisée. Leur protection dépend donc uniquement des solutions de sécurité qui étaient déjà installées, ou pas.

D'autre part, l'équipe informatique n'administre pas directement ces machines via le réseau. Elle est obligée de faire confiance aux utilisateurs pour ce qui est du respect des protocoles de sécurité et de l'installation systématique des mises à jour nécessaires. Son plus gros problème dorénavant est de comprendre les équipements qui se connectent au réseau, leurs vulnérabilités et, surtout, de déployer les correctifs sur ces centaines voire milliers de points d'extrémité distants, via des réseaux privés virtuels et avec une bande passante réseau limitée. En cas de problème, le personnel informatique ne peut pas se rendre dans le bureau du collaborateur concerné comme il le ferait en temps normal.

**La gestion des vulnérabilités va-t-elle aussi évoluer ? Si oui, comment ?**
**Marco Rottigni –** Le nombre de vulnérabilités logicielles augmente chaque jour. La multiplication des failles découvertes tant dans des logiciels utilisés depuis des années qu'au sein d'applications plus récentes fait que le déploiement de tous les correctifs reste compliqué.

Des éditeurs majeurs tels que Microsoft et Adobe publient des correctifs une fois par mois pour

faciliter les choses. Regrouper des correctifs dans le cadre de publications mensuelles est censé permettre au service informatique de tester plus facilement les mises à jour et également de veiller à leur installation. Mais cette logique ne vaut que lorsque ce même service informatique a le plein contrôle sur le réseau et sur l'équipement en question. Elle laisse le temps de tester les nouveaux correctifs pour vérifier qu'ils ne fragilisent pas d'autres composants logiciels, puisque tous les équipements vulnérables sont en partie protégés par le firewall de l'entreprise. Elle permet également de vérifier que les mises à jour ont été bien installées et d'aviser dans le cas contraire.

Les choses ne sont plus si simples dans le contexte actuel. En effet, pour les équipements personnels des collaborateurs, les niveaux de sécurité à imposer avant d'accorder un accès doivent être gérés avec attention. Pour les équipements d'entreprise qui se trouvent actuellement en dehors du réseau, il n'est pas évident non plus de savoir ce qui a été installé et mis à jour sur ces derniers. Enfin, Il se peut que ces points d'extrémité soient aujourd'hui moins protégés contre les attaques.

Les remontées d'information sont indispensables. Par le biais de services Cloud, le service informatique pourra connaître l'état actuel de chaque machine utilisée par les collaborateurs, ce qui lui donnera un aperçu des nouvelles vulnérabilités découvertes et lui permettra d'afficher ensuite tous les actifs ayant le même profil. En outre, toute nouvelle approche devra permettre au service informatique d'automatiser le déploiement des correctifs pour que les équipements reçoivent automatiquement les mises à jour et restent sécurisés dans la durée. Enfin, l'équipe IT doit pouvoir définir ses propres règles pour hiérarchiser le déploiement des correctifs, après avoir classé les nouveaux problèmes en fonction de leur gravité, de leur niveau de risque et de leur exploitation potentielle.

Parallèlement, le déploiement des patches devra s'effectuer à distance. Plutôt que de s'en remettre aux employés et à leur aptitude à déployer les mises à jour, le contrôle et la gestion centralisés des correctifs par le service informatique garantiront le bon déploiement des correctifs. Cette approche assure la cohérence de la conformité et de la sécurité face aux problèmes tout en facilitant le déploiement de correctifs en cas de découverte de nouvelles menaces notoires qui risqueraient sinon de compromettre les actifs et les données de l'entreprise.

**Avec le déconfinement, on se prépare à un retour à la normale ?**
**Marco Rottigni –** Le principal défi pour la sécurité n'est pas uniquement le contexte actuel du télétravail, mais aussi ce qui se passera ensuite, dans les prochaines semaines et dans les mois à venir. Pour soutenir le travail à distance, il faut pouvoir disposer dans la durée du même niveau d'information pertinent sur tous les actifs et équipements de l'entreprise que celui fourni par le réseau de l'entreprise. À défaut, il sera impossible de maintenir le bon niveau de visibilité et de sécurité.

Concernant le travail intelligent, il est possible de rationaliser et d'améliorer ces processus pour que le travail se déroule sans heurt et plus facilement. Des outils en ligne peuvent servir à reproduire l'environnement antérieur chaque fois que cela se justifie, à éliminer les problèmes chaque fois que possible et à préserver la sécurité de l'ensemble du processus. Sans oublier que certains télétravailleurs exigeront davantage d'attention et de soutien que d'autres pour assurer la protection de leur système.

Il donc est primordial de chercher à comprendre les risques de vulnérabilités à mesure qu'ils apparaissent, comment il est possible d'y remédier et comment gérer la réponse à l'échelle de l'entreprise. Cette nouvelle approche est indispensable pour sécuriser le télétravail et rendre l'environnement de travail actuel le plus proche possible de l'activité habituelle.