Livre blanc

Rapport Cisco Connected World sur la sécurité mobile : *Résultats de l'étude et questions que doivent se poser les services informatiques*

Synthèse

Pour mieux comprendre les problèmes croissants de sécurité liés à l'intégration des appareils mobiles aux activités de l'entreprise, Cisco a récemment mené une étude portant sur les comportements et les expériences d'utilisateurs du monde entier. L'étude *Cisco Connected World sur la sécurité mobile* aborde divers sujets :

- l'attitude des employés vis-à-vis de l'utilisation d'appareils personnels (leur appartenant) ou fournis par l'entreprise pour accéder aux réseaux d'entreprise,
- les types d'appareils personnels et fournis par l'entreprise utilisés pour accéder au réseau,
- le comportement en ligne des employés utilisant des appareils mobiles,
- la perception qu'ont les employés de la sécurité des appareils mobiles.

Alors que le nombre d'appareils mobiles ne cesse d'augmenter sur le lieu de travail, les départements informatiques et les entreprises pour qui ils travaillent peuvent exploiter ces résultats pour déterminer le meilleur moyen de permettre aux employés d'accéder au réseau de manière productive, flexible et sécurisée avec tout type d'appareil.

Introduction

La mobilité d'entreprise et la « consumérisation de l'informatique » (utilisation par les employés d'appareils personnels et d'applications cloud dans l'entreprise) se sont déjà bien développées dans le monde. Mais les départements informatiques, notamment ceux de grands groupes, luttent pour rester à la page et relever les défis que ces tendances engendrent : la détérioration du périmètre de sécurité traditionnel, la prolifération de terminaux devant être sécurisés et des employés de plus en plus demandeurs d'un accès permanent et en tout lieu aux ressources de l'entreprise avec les appareils mobiles de leur choix.

Les administrateurs informatiques sont mis au défi de trouver l'équilibre optimal entre sécuriser les données confidentielles de l'entreprise et permettre aux employés d'accéder aux outils et aux informations dont ils ont besoin pour travailler. Les appareils mobiles, et donc les données et les informations d'identification d'accès qu'ils contiennent, se perdent et se volent facilement. Les employés qui transfèrent des données vers des appareils mobiles via des réseaux publics peuvent compromettre la sécurité des informations confidentielles de l'entreprise. En outre, les utilisateurs qui accèdent à Internet à partir de leur appareil mobile sont constamment exposés à des menaces Web, notamment les programmes malveillants qui volent des données.

Toutefois, il est impératif de trouver le juste équilibre, car il ne s'agit pas uniquement d'un problème de sécurité. L'intégration des technologies mobiles au sein des activités de l'entreprise offre une plate-forme favorisant l'innovation continue et à moindre coût et par là même la collaboration et la productivité des employés. Dans un

monde toujours plus connecté, l'adoption des technologies mobiles permettra aux entreprises non seulement de rester compétitives, mais également d'attirer et de conserver les plus grands talents.

Le rapport « *Cisco Connected World Technology* »[1] s'intéressait à l'origine aux changements d'attitude des étudiants et des jeunes professionnels (nouvelle génération d'employés et d'utilisateurs) du monde entier vis-à-vis du travail, de la technologie et de la sécurité. L'étude a été étendue aux employés de tous âges et montre que les entreprises n'ont pas encore complètement appliqué toutes les procédures élémentaires de sécurité, tant en ce qui concerne les appareils mobiles que l'accès à distance aux données de l'entreprise. Il apparaît clairement que les sociétés doivent se concentrer davantage sur la création et la mise en œuvre de politiques à la fois robustes et flexibles. Elles doivent également informer les utilisateurs des menaces potentielles et les sensibiliser aux bonnes pratiques à mettre en œuvre pour les éviter.

Utilisation d'appareils personnels ou fournis par l'entreprise dans le cadre d'activités professionnelles

Les résultats de l'étude *Cisco Connected World sur la sécurité mobile* indiquent que les sondés utilisent quotidiennement pour leur travail et dans des proportions quasi identiques des appareils personnels ou fournis par l'entreprise, qu'il s'agisse d'ordinateurs portables, d'ordinateurs de bureau, de smartphones ou de tablettes. Certains d'entre eux utilisent plusieurs de ces appareils.

Ces résultats indiquent incontestablement que l'utilisation d'un appareil personnel à des fins professionnelles est de plus en plus répandue. En effet, environ la moitié (45 %) des sondés affirment que leur employeur préfère leur attribuer un budget fixe pour acheter leur propre ordinateur portable, smartphone ou autre appareil de leur choix, plutôt que fournir le même équipement à tout le monde. La plupart des employeurs prennent également en charge les abonnements aux solutions voix et/ou données pour les appareils personnels que leurs employés utilisent au travail.

Plus de la moitié participants à l'enquête ont répondu qu'ils souhaiteraient pouvoir utiliser les appareils fournis par l'entreprise à des fins personnelles. En outre, pratiquement tous les sondés aimeraient pouvoir accéder aux mêmes applications, fonctionnalités de bureau et données, et bénéficier de la même expérience utilisateur, que l'appareil soit personnel ou fourni par l'entreprise.

Question que doit se poser le service informatique :

- Comment protéger les applications et les données sur tous les appareils ?

Accès à distance transparent

Selon l'étude *Cisco Connected World sur la sécurité mobile*, les entreprises semblent faire des efforts pour prendre en charge le nombre croissant d'utilisateurs mobiles et de télétravailleurs. Plus de la moitié des sondés déclarent pouvoir actuellement se connecter sans problèmes à leur réseau d'entreprise, en tout lieu et à tout moment. Sur l'ensemble des participants à l'enquête, ce sont les utilisateurs du Brésil, d'Inde et des États-Unis qui ont le moins de difficulté à accéder à distance à leur réseau d'entreprise. Cela peut indiquer que leurs employeurs offrent une connectivité sécurisée aux télétravailleurs et aux utilisateurs mobiles. Mais cela peut également vouloir dire le contraire.

Fait intéressant, alors que la plupart des sondés considèrent que l'accès à distance est un privilège et non pas un droit, nombre d'entre eux ont des attentes élevées en matière de connectivité à distance et se plaignent de la mauvaise qualité des connexions fournies par leurs employeurs. En particulier, les utilisateurs vivant en Chine, dont beaucoup considèrent l'accès à distance comme un droit, ont cité les restrictions d'accès au réseau comme

[1] Rapport « Cisco Connected World Technology 2012 » : http://www.cisco.com/en/US/netsol/ns1120/index.html.

leur principale frustration. D'autres ont cité les politiques de l'entreprise, les restrictions budgétaires et la réglementation comme les principaux obstacles à un accès à distance de qualité.

Question que doit se poser le service informatique :

- Comment sécuriser les connexions des télétravailleurs sans compromettre l'expérience utilisateur ?

Connexions sécurisées

Alors qu'un nombre croissant d'employés demandent à utiliser l'appareil de leur choix dans l'entreprise, beaucoup reconnaissent également que le BYOD fait courir des risques à leur employeur. La majorité des sondés pensent qu'un smartphone personnel connecté à Internet présente un plus grand risque pour la sécurité qu'un smartphone fourni par l'entreprise.

Environ la moitié (46 %) d'entre eux estiment qu'une connexion filaire à un ordinateur portable est le moyen le plus sûr de se connecter à distance. Toutefois, 60 % des sondés ont également déclaré emprunter au moins occasionnellement la connexion sans fil d'un tiers lorsqu'ils travaillent à distance (à noter que la moitié des utilisateurs en Inde déclarent emprunter « systématiquement » la connexion d'un tiers). L'absence d'une autre connexion Internet et la facilité sont les deux principales raisons pour emprunter des connexions sans fil.

Questions que doit se poser le service informatique :

- Comment garantir un accès à distance sécurisé à partir de connexions sans fil ?
- Comment garantir un accès sécurisé et homogène aux utilisateurs d'appareils personnels ou fournis par l'entreprise ?

Comportements en ligne et menaces

Les résultats de l'étude *Cisco Connected World sur la sécurité mobile* indiquent que, même s'ils sont conscients des risques que la mobilité pose à la sécurité de l'entreprise, la plupart des employés adoptent tout de même un comportement à risque lorsqu'ils utilisent leurs appareils mobiles. En fait, 26 % des participants à l'enquête affirment prendre davantage de risques avec un appareil fourni par l'entreprise qu'avec leur propre appareil. En effet, celles qui reconnaissent adopter un comportement plus risqué en se connectant à Internet à partir d'un appareil fourni par l'entreprise pensent que le service informatique les aidera en cas de problème. (Les employés se comportent probablement ainsi parce qu'ils pensent que le logiciel de protection contre les menaces les protégera.) Voici quelques exemples de comportements à risque :

- **L'utilisation d'applications collaboratives :** 40 % des sondés déclarent utiliser des applications collaboratives (voix, vidéo et conférences Web, notamment) mobiles, de messagerie et de réseau social d'entreprise sur les appareils mobiles qu'elles utilisent à des fins professionnelles. Souvent, les applications collaboratives sont basées sur le Web. Mais le service informatique de l'entreprise ne contrôle pas toujours leur utilisation ou ne sait pas que les employés s'en servent. Les personnes interrogées, notamment en Chine, qui n'utilisent pas d'applications collaboratives sur leurs appareils personnels ni ceux fournis par l'entreprise, considèrent généralement les problèmes de sécurité comme le principal obstacle.
- **Le téléchargement de données confidentielles de l'entreprise sur un appareil mobile :** 63 % des sondés reconnaissent télécharger certaines données confidentielles de l'entreprise sur leur ordinateur personnel ou leur appareil mobile, au moins occasionnellement. Ce phénomène est plus marqué et plus fréquent dans certains pays, notamment en Inde, où 58 % des utilisateurs téléchargent « tout le temps » des données confidentielles de l'entreprise. Dans tous les pays couverts par cette étude, les personnes

interrogées qui ont cette attitude déclarent le faire parce qu'elles « [doivent] avoir ces informations, quel que soit l'endroit où [elles se trouvent], que la connexion soit sécurisée ou non ».

- **L'absence de protection des données téléchargées sur un appareil mobile :** environ 10 % des sondés ont déclaré ne pas prendre de mesure pour protéger les données qu'ils téléchargent sur leur appareil mobile sans fil. La principale raison de ce comportement a été clairement identifiée : environ la moitié de ceux qui ont affirmé ne jamais recourir au cryptage ou à la définition de mots de passe sur leur appareil sans fil ne savent pas comment faire. Une meilleure formation des utilisateurs pourrait facilement résoudre ce problème.

Les menaces Web constituent une autre source importante de préoccupation en termes de sécurité : environ la moitié des personnes interrogées ont déjà été victimes (virus ou hameçonnage, par exemple) sur un appareil fourni par l'entreprise. Les utilisateurs d'appareils personnels sont encore plus nombreux à avoir rencontré des menaces Web. La menace que présentent les téléchargements de logiciels malveillants sur le Web semble être moins répandue. Seulement un tiers des sondés ont déjà téléchargé des logiciels malveillants sur leur appareil personnel ou celui fourni par l'entreprise.

Au sujet des alertes de sécurité : lorsqu'un message d'avertissement s'affiche sur leur appareil personnel ou celui fourni par l'entreprise, la plupart des personnes interrogées déclarent avoir cliqué dessus, puis lu attentivement les informations affichées avant de décider ce qu'elles allaient faire. (Cependant, les personnes interrogées en Inde et au Royaume-Uni semblent globalement être moins prudentes que les utilisateurs des autres pays dans lesquels l'étude a été réalisée, car elles acceptent les messages d'avertissement sans lire leur contenu.)

Questions que doit se poser le service informatique :

- Comment faire pour que les utilisateurs d'appareils mobiles adoptent la « bonne attitude » ?
- Comment protéger les données de l'entreprise sur les appareils personnels des employés ?
- Les avertissements de sécurité adressés aux employés sont-ils efficaces ?
- La formation dispensée aux utilisateurs est-elle suffisante ?

Appareils perdus ou volés

La perte d'un appareil personnel ou fourni par l'entreprise, utilisé à des fins professionnelles, peut avoir de graves conséquences sur la sécurité. Cela risque notamment de se traduire par une perte de données intellectuelles qui peut ternir la réputation de l'entreprise, dévaloriser sa marque ou compromettre son avantage concurrentiel. La violation des règles de conformité en termes de sécurité des données constitue une autre source de préoccupation majeure pour les entreprises, car elles peuvent ébranler la confiance des clients, entraîner des pénalités coûteuses et avoir des répercussions juridiques.

Pourtant, 60 % des employés ayant participé à l'étude *Cisco Connected World sur la sécurité mobile* disent avoir récemment pris des risques en utilisant un appareil à des fins professionnelles. Emprunter la connexion sans fil d'un tiers alors qu'ils travaillent à distance ou à domicile, autoriser une personne étrangère à l'entreprise à utiliser leur appareil professionnel ou laisser leur appareil à la vue de tous dans une voiture font partie des comportements à risque les plus fréquents chez ces employés. Ces 12 derniers mois, pratiquement la moitié des personnes interrogées ont perdu ou se sont fait voler un PDA ou une tablette (personnel ou fourni par l'entreprise) utilisé à des fins professionnelles. Plus d'un tiers d'entre elles ont perdu ou se sont fait voler leur smartphone ou celui fourni par l'entreprise.

Globalement, les personnes interrogées pensent que perdre un appareil fourni par l'entreprise est un peu plus risqué que de perdre un appareil personnel utilisé à des fins professionnelles. Pour environ deux tiers d'entre elles, perdre leur propre appareil ou celui fourni par l'entreprise hors du lieu de travail, inscrire leurs codes d'accès sur un bout de papier ou laisser un appareil à la vue de tous dans une voiture sont les principaux risques qu'une entreprise peut courir en matière de sécurité.

Question que doit se poser le service informatique :

- Quel type de contrôle exercer sur les appareils s'ils sont perdus ou volés ?

Préoccupations face aux menaces à la sécurité

La plupart des sondés semblent admettre que la perte d'un appareil hors du lieu de travail ou les comportements risquant de compromettre les appareils ou les codes d'accès peuvent nuire à la sécurité de l'entreprise. Pourtant, les résultats de l'étude indiquent que peu d'utilisateurs se soucient de la sécurité des appareils, qu'ils leur appartiennent ou qu'ils soient fournis par leur employeur.

Dans l'ensemble, les personnes interrogées dans le cadre de l'étude *Cisco Connected World sur la sécurité mobile* avancent plusieurs raisons de ne pas se sentir toujours concernées par les menaces à la sécurité. La principale raison est que le risque leur semble trop faible pour les inquiéter. Certains sondés ont précisé qu'ils ne se sentaient pas toujours concernés par la sécurité des appareils, car le service informatique de leur entreprise ne les avait pas informés de ces menaces.

Questions que doit se poser le service informatique :

- Comment mieux faire connaître les menaces potentielles pour la sécurité des appareils ?

Attitudes des employés vis-à-vis de l'informatique au travail

Les résultats de l'étude *Cisco Connected World sur la sécurité mobile* révèlent que les politiques et les procédures appliquées par les entreprises pour se protéger contre les menaces varient considérablement. Et même s'ils existent, les accords de sécurité sont parfois ignorés, non appliqués, voire inefficaces.

58 % des personnes interrogées déclarent avoir signé des accords de sécurité spécifiques concernant les données internes lors de leur arrivée dans l'entreprise. Alors que 77 % d'entre elles affirment se conformer strictement à ces accords, environ un quart avoue ne pas toujours respecter les politiques de l'entreprise. 42 % des personnes qui ne respectent pas toujours l'accord de sécurité de leur entreprise précisent qu'elles « oublient parfois » de le faire.

Les résultats de l'étude indiquent que 84 % des personnes interrogées pensent que leur service informatique est capable d'identifier les menaces à la sécurité. Plus de la moitié des personnes interrogées affirment que leur service informatique dispense régulièrement une formation sur les risques et les contrôles de sécurité. Par ailleurs, environ la moitié des personnes interrogées déclarent que leur service informatique joue un rôle proactif en les avertissant à temps des menaces et des risques potentiels. Finalement, trois quarts d'entre elles disent être devenus plus prudents.

Questions que doit se poser le service informatique :

- Comment appliquer notre politique ?
- La formation dispensée aux utilisateurs est-elle efficace et opportune ?

Conclusion

Comme l'indiquent les résultats de l'étude *Cisco Connected World sur la sécurité mobile*, la mobilité représente des enjeux complexes pour les entreprises et les services informatiques du monde entier. Garantir une « mobilité sécurisée » n'est pas chose aisée. Chaque entreprise doit développer une approche mixte de la sécurité mobile alliant politiques, formation et technologie, qui répondra aux besoins de son personnel tout en l'aidant à rester productif et à atteindre les principaux objectifs de l'entreprise. Et cela prendra probablement du temps... [2][3]

Parallèlement, beaucoup d'entreprises font beaucoup d'efforts non seulement pour adapter leur modèle de sécurité afin de répondre aux besoins du monde connecté, mais également pour essayer de trouver un terrain d'entente avec les employés qui veulent pouvoir accéder aux applications avec les appareils de leur choix. Alors qu'elles tentent de trouver les « meilleures » réponses aux multiples questions et enjeux évoqués dans ce livre blanc, elles réévaluent leurs codes de conduite commerciale et leurs politiques d'utilisation acceptable en mettant davantage l'accent sur la prévention des pertes de données et en œuvrant pour placer la sécurité de l'entreprise au premier rang des préoccupations de tous les employés et à tous les niveaux.

Accès sécurisé Cisco

La solution d'accès sécurisé de Cisco peut aider les entreprises et leur service informatique à répondre à la demande croissante des employés en matière de mobilité et de choix d'appareil tout en minimisant les risques pour la sécurité grâce à la création d'une base permettant aux utilisateurs de se connecter à tout moment, où qu'ils soient, et quel que soit l'appareil. Elle favorise le développement du BYOD, de la collaboration et du cloud et contribue à transformer l'espace de travail en toute confiance.

- Une infrastructure unifiée régie par des règles permet aux appareils et aux utilisateurs de se connecter de manière sécurisée et homogène au réseau de l'entreprise (filaire, sans fil ou VPN).
- Des couches supplémentaires sont indispensables pour garantir une sécurité efficace ainsi qu'une expérience favorisant la productivité des utilisateurs aussi bien sur site que hors site.
- La solution est dotée d'une interface de gestion simplifiée offrant une visibilité globale grâce à laquelle le dépannage est plus rapide. Les entreprises peuvent ainsi davantage se consacrer à l'innovation, en toute confiance.

La solution d'accès sécurisé allie des composants performants : le client pour la mobilité sécurisée Cisco AnyConnect®, les pare-feu Cisco de nouvelle génération ASA 5500-X, le moteur Cisco Identity Services Engine (ISE) et Cisco TrustSec®.

Pour plus d'informations sur notre solution d'accès sécurisé et ses composants, visitez le site Web http://www.cisco.com/en/US/netsol/ns1204/index.html - ~Products.

Solution Cisco pour le BYOD

Cisco ouvre la voie du BYOD aux entreprises et propose des options de déploiement souples pour les solutions de mobilité/BYOD et un choix simple de plates-formes ou de services.

Cisco propose également une approche complète en matière de conception, de gestion et de contrôle d'accès à un réseau BYOD. La solution Cisco pour le BYOD offre aux entreprises l'un des systèmes de gestion des terminaux et

[2] Vous pouvez télécharger les rapports annuels 2011 et 2013 de Cisco sur la sécurité à partir du site : http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html.
[3] Rapport annuel 2013 de Cisco sur la sécurité : http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html..

du cycle de vie du réseau les plus sécurisés et complets du marché. Elle simplifie les opérations informatiques grâce à la gestion de bout en bout du cycle de vie du réseau. Elle procure une expérience utilisateur sans concession, laissant chacun travailler comme il l'entend. Enfin, elle permet aux entreprises de protéger leurs données grâce à des politiques unifiées et à des contrôles indispensables à la prise en charge de l'environnement de travail « au-delà du BYOD ».

En savoir plus sur la solution Cisco pour le BYOD.

Initiative « Tout appareil » de Cisco

Cisco fait partie des nombreuses entreprises qui œuvrent au développement de solutions de mobilité sécurisée pour tous les utilisateurs, où qu'ils soient et quel que soit l'appareil qu'ils souhaitent utiliser. À l'heure actuelle, Cisco gère plus de 64 000 appareils mobiles. Les employés ont la possibilité de choisir leur appareil et de le connecter en toute sécurité à des services vocaux, vidéo et de données, où qu'ils soient, conformément à la politique d'utilisation « Tout appareil ».

Le développement du programme BYOD de Cisco a été analysé dans les deux derniers *rapports annuels de Cisco sur la sécurité*.[2] Lorsque Cisco atteindra la dernière étape du programme BYOD, dans quelques années, la société sera de plus en plus indépendante des sites d'activité et des services, mais la sécurité de ses données sera préservée.[3]

MÉTHODOLOGIE

L'étude *CCsco Connected World sur la sécurité mobile* a été menée par Cisco en 2012 dans 10 pays, dans la langue locale, auprès de 4 600 personnes répondant aux critères suivants :

- Résider dans les pays suivants : Allemagne, Australie, Brésil, Chine, États-Unis, France, Inde, Italie, Japon ou Royaume-Uni
- Avoir au moins 21 ans
- Être employé permanent
- Travailler pour une entreprise d'au moins 10 employés
- Ne pas travailler dans un cabinet d'études commerciales, dans une société de conseil en informatique ou dans une organisation à but non lucratif
- Utiliser des appareils personnels ou fournis par l'entreprise pour le travail
- Travailler à distance quelques fois par an

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose. CA

Siège social en Asie-Pacifique
Cisco Systems (États-Unis) Pad Ltd.
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam,
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et de fax sont répertoriés sur le site Web de Cisco, à l'adresse : www.cisco.com/go/offices.

Imprimé aux États-Unis C11-728986-01 08/13