

Une étude sur le comportement des utilisateurs distants

Introduction

En ces temps où une des préoccupations majeures des entreprises est d'empêcher la fuite d'information – volontaire ou involontaire –, l'attention se focalise toujours plus autour du maillon souvent considéré comme le plus faible en sécurité : les utilisateurs finaux, et en particulier les utilisateurs nomades. L'explosion de la population nomade dans les entreprises est un fait, ainsi que l'augmentation de la quantité (et de la criticité) des informations qui sont mises à leur disposition, et stockées sur des équipements divers, tels des PC portables mais également téléphones 3G. La mobilité des collaborateurs d'une entreprise permet d'être plus productif, plus réactif, plus « agile » et souvent également d'offrir une satisfaction plus grande pour l'employé. Il est désormais possible de travailler d'où on le souhaite, à n'importe quel moment, et avec des outils variés.

Bien évidemment, cette mobilité introduit des risques importants : les outils avec lesquels l'employé se connecte ne sont pas, par essence, reliés en permanence au réseau de l'entreprise, et donc ne bénéficient pas des outils de sécurité déployés (qu'il s'agisse de la distribution des correctifs de sécurité, des mises à jour anti-virus, mais aussi des outils de sécurité périmétrique – filtrage de contenu, firewall...), voire ces équipements n'appartiennent pas à l'entreprise (dans le cas, par exemple, d'un portail SSL accédé depuis un ordinateur en libre accès dans un hall d'hôtel ou depuis l'ordinateur familial). Ces populations sont souvent les premières touchées par les incidents de sécurité.

Dans un processus de gestion des risques, il est donc important de connaître et de comprendre le comportement des utilisateurs nomades et leur perception de la sécurité. Armées de cette connaissance, les directions informatiques, directions de la sécurité de l'information, peuvent prendre les décisions – qui peuvent être d'ordre technologique, comme le déploiement d'un outil de sécurité sur les postes mobiles ou non technologiques, comme des actions de sensibilisation – qui s'imposent pour aborder de manière proactive les menaces pesant sur cette population. Mais on ne dispose finalement que de peu d'informations sur le sujet. Toutes les entreprises ne voulant ou ne pouvant s'offrir des audits de sécurité comprenant une brique d'ingénierie sociale testant – anonymement ou non – le comportement des utilisateurs, Cisco a commandité une étude à l'organisme Insightexpress, dont l'intégralité des résultats se retrouve sur Cisco.com (lien en annexe).

Cette étude, sous forme de questionnaire, a été effectuée en parallèle dans une dizaine de pays, dont la France, et permet donc de sortir quelques données spécifiques à notre pays.

Les pays audités sont : Etats-Unis, Angleterre, France, Allemagne, Italie, Japon, Chine, Inde, Australie et Brésil.

La conscience des enjeux

La conscience de l'existence de problématiques de sécurité liées à la mobilité est une première étape cruciale dans le processus de protection d'une organisation. L'étude globale montre que la majorité (66%) des personnes interrogées – travailleurs nomades - a conscience d'un enjeu de sécurité. La France se situe dans la moyenne, à 65%.

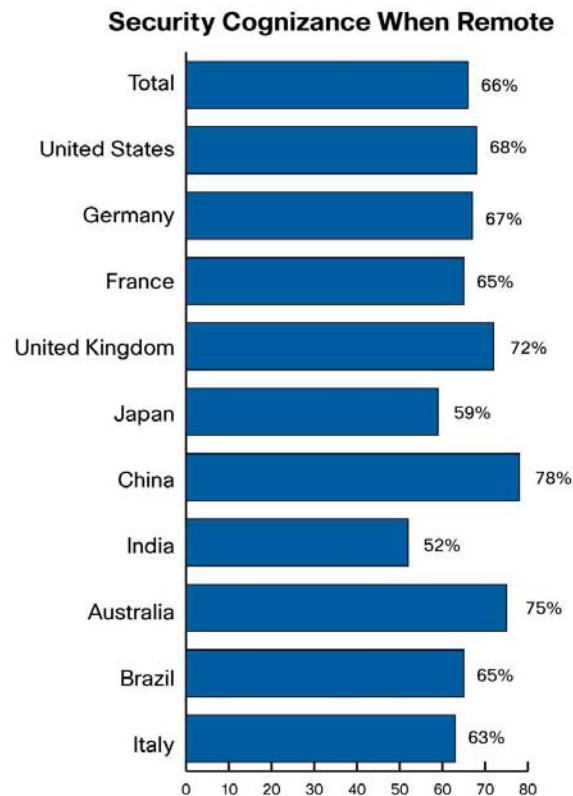


Figure 1 : Les utilisateurs affirment être conscients de l'importance de la sécurité lorsqu'ils travaillent à distance.

Malheureusement, bien que les utilisateurs aient conscience de l'importance de la sécurité, cette connaissance n'est pas suffisante pour assurer un comportement discipliné parmi les travailleurs mobiles. Qu'un utilisateur pense ou dise qu'il a conscience des enjeux ne signifie pas qu'il sait comment se comporter pour assurer un bon niveau de sécurité. Et un employé qui n'est pas au courant des bonnes pratiques à appliquer dans une telle situation mais qui pourtant croit bien faire, peut faire augmenter grandement le niveau de risque. Afin d'étudier le lien entre ce que pensent les utilisateurs et leur comportement, l'étude a inclus une série de questions portant sur ce dernier. Et la perception joue un rôle fondamental dans la façon dont les utilisateurs se comportent : les utilisateurs pensent bien se comporter (par rapport aux risques de sécurité) et pourtant font courir des dangers. Un exemple ? Environ un tiers (29 %) des personnes interrogées utilisent l'ordinateur de l'entreprise pour leur usage personnel. Et cela ne pose pas que des défis en terme de productivité mais également en terme de sécurité.

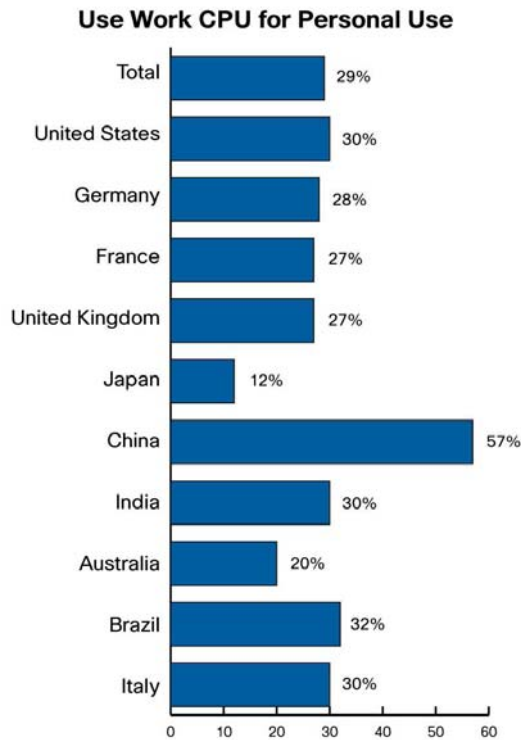


Figure 2: Un nombre significatif d'utilisateurs utilisent leur ordinateur à des fins personnelles.

Un autre exemple, sans doute plus significatif, est celui du prêt de l'ordinateur : évidemment, prêter son ordinateur portable à un utilisateur ne faisant pas partie de l'entreprise est une invitation à de futurs problèmes de sécurité, les utilisateurs externes n'ayant pas été éduqués aux problématiques de sécurité et n'étant pas tenus au respect des politiques internes à l'organisation. Et pourtant, l'étude révèle qu'un nombre significatif d'utilisateurs partagent leur ordinateur avec d'autres. Et cela malgré leur conscience globale de l'existence d'enjeux autour de la sécurité...

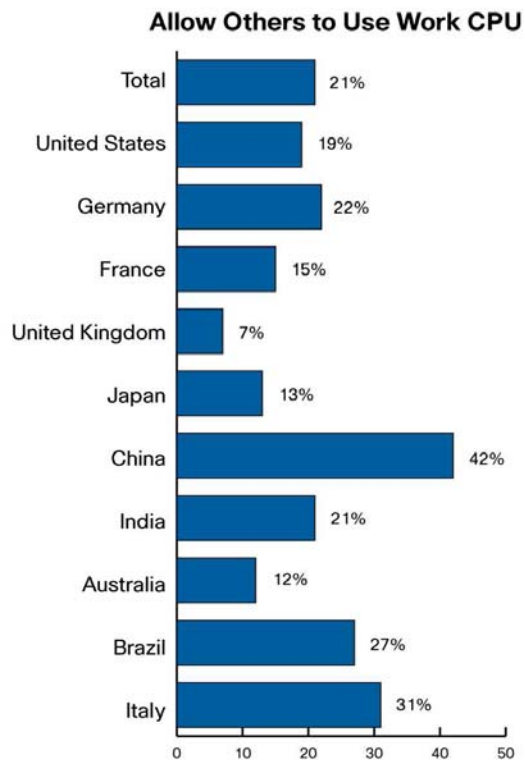


Figure 3: Un nombre significatif des utilisateurs interrogés autorise d'autres personnes à utiliser leur ordinateur professionnel.

Encore une fois, l'ignorance des risques semble guider ce type de comportement : 37% des télétravailleurs qui partagent leur ordinateur avec d'autres – famille, amis – disent qu'ils ne voient rien de mal à cela. 26% pensent que cela n'augmente pas le risque en terme de sécurité. Et plus d'un télétravailleur sur trois (35%) partageant son ordinateur avec d'autres affirme que ce partage « ne dérange pas l'entreprise »... Il est peut être temps de réviser les politiques de sécurité, ou plutôt de communiquer plus efficacement avec cette population....

De nombreux utilisateurs admettent ainsi implicitement avoir un comportement à risque. Mais il n'y a pas que le prêt de l'ordinateur : regardons maintenant du côté e-commerce, du wifi, et des emails... Le fossé se creuse entre la prétendue conscience de la nécessité d'appliquer certaines bonnes pratiques et la réalité

Online Shopping

Une majorité des télétravailleurs (71%) affirment qu'ils n'utilisent pas leur ordinateur professionnel pour un usage personnel. Mais 40% de ces mêmes personnes disent utiliser leur ordinateur professionnel pour faire du shopping sur Internet. Pourquoi faire ce shopping sur Internet pendant que l'on travaille à distance ? Les réponses varient :

Pourquoi faire du shopping sur Internet depuis l'ordinateur professionnel ? Parce que...

Je n'aurai jamais le temps de faire ces activités hors de mon temps de travail	43%
Le shopping en ligne ne peut pas poser de problème de sécurité	22%
Mon PC professionnel est plus sécurisé que mon pc personnel	21%
C'est ok tant que mon chef ne le sait pas	9%
Les autres le font bien !	18%
Cela ne dérange par mon organisation	49%
J'imagine que ca ne dérange pas mon organisation	24%
Je doute que l'entreprise puisse s'en rendre compte	7%
L'IT interne m'aidera si j'ai un problème lors de la transaction	16%

Figure 4: La majorité des utilisateurs font du shopping sur internet car "cela ne pose pas de problème à l'entreprise" et ils "n'auraient jamais le temps de le faire s'ils ne le faisaient pas sur les horaires de travail".

Certaines de ces réponses démontrent des lacunes dans la connaissance des risques liées à ce type de comportement....

Le Wifi

Une autre surprise provient du fait qu'un utilisateur sur dix affirme qu'il a déjà utilisé une connexion wifi non sécurisée appartenant à un voisin. Et 20% des personnes interrogées ne sont pas capables de dire si, lorsqu'elles travaillent de chez elles, elles sont bien connectées à leur réseau wifi et pas à celui du voisin.

Un autre groupe (18%) affirme d'ailleurs que « tant que le voisin ne le sait pas, c'est bon ». Encore une fois, comme pour le shopping sur Internet, certains utilisateurs se sentent plus concernés par le gain de temps que par la sûreté.

Les équipements personnels

Le fait que les utilisateurs se connectent aux ressources de l'entreprise au travers d'équipements

personnels pose des risques sérieux. La plupart du temps, ces équipements ne répondent pas aux bonnes pratiques en terme de sécurité, comme la présence d'un anti-virus à jour. Hors, 45% des personnes interrogées affirment utiliser parfois leurs propres équipements pour accéder à des ressources de l'entreprise. Certaines pensent que c'est tout à fait acceptable, simplement parce que cela fait longtemps qu'elles le font sans que cela ne pose de problème apparent.

Le comportement vis à vis de l'email

L'email est depuis longtemps maintenant un vecteur important d'infection des entreprises par des vers, virus, chevaux de Troie, et de plus en plus utilisé pour le vol de données. La plupart des utilisateurs sont conscients du risque lié à l'email, mais un nombre surprenant d'utilisateurs (3% en France) ouvrent les messages ET les attachements des mails provenant d'une source inconnue... 3%, cela représente 30 personnes dans une entreprise de 1000 employés ! Ce taux est donc bien trop élevé et inacceptable pour la plupart des organisations.

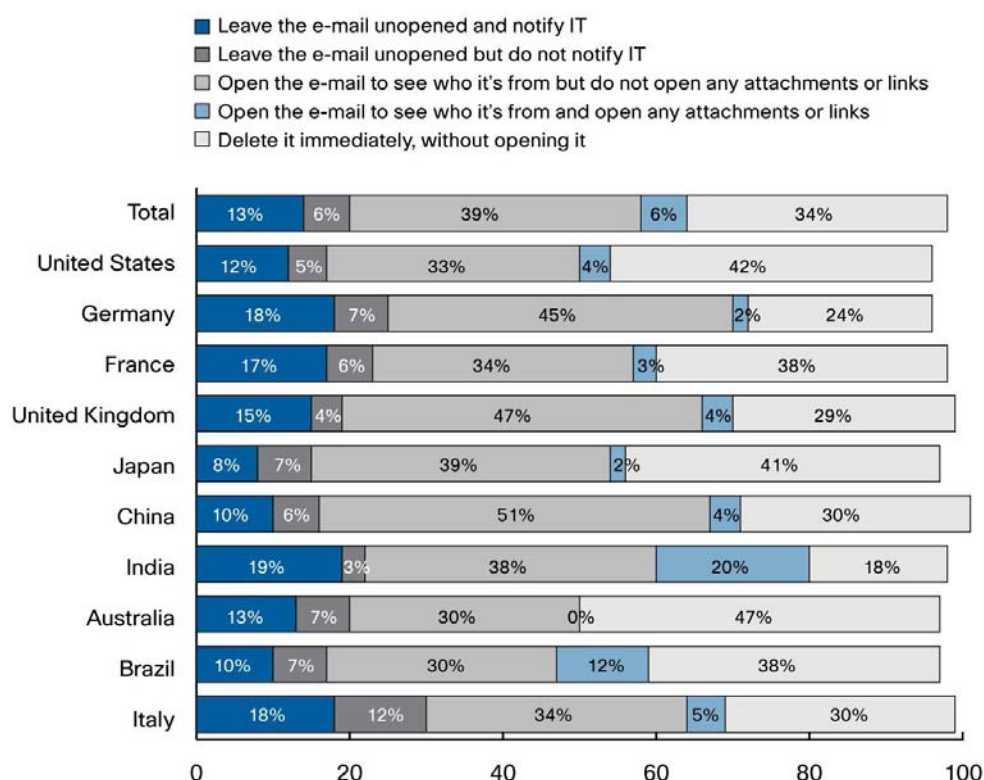


Figure 5: Le comportement des utilisateurs face aux emails de sources inconnues.

38 % des utilisateurs ouvrent le mail mais pas la pièce jointe : un comportement certes moins risqué qu'en ouvrant la pièce jointe, mais tout de même risqué, quand on pense au nombre de vulnérabilités day0 qui peuvent parfois être exploitées.

Transférer des fichiers du PC personnel dans l'environnement de l'entreprise est également une activité à risque (surtout si on corrèle cette information avec le fait qu'une proportion non négligeable des télétravailleurs considère le PC professionnel plus sécurisé, ce qui implicitement indique qu'ils doutent du bon niveau de sécurité de leurs actifs propres), qui pourtant est réalisée par 46% des utilisateurs.

Il est impossible de terminer cette analyse sans rappeler ce formidable exercice réalisé par les organisateurs d'Infosecurity Europe en 2004 dans le métro de Londres : les organisateurs ont proposé à 172 travailleurs une barre de chocolat s'ils révélaient leur mot passe. 37% ont immédiatement accepté, et 34% l'ont fait après que l'interviewer ait dit qu'il s'agissait probablement du nom de leur enfant ou de leur animal de compagnie.... Mais c'était en 2004, et même s'il est probable que des réels progrès ont été effectués, cela donne une mesure du chemin qu'il reste à parcourir !

Le défi et les opportunités

La contradiction entre le sentiment de conscience des enjeux et le comportement réel des utilisateurs nomade pose un réel défi aux équipes sécurité. Clairement, ce constat impose une meilleure communication des équipes IT vers les utilisateurs finaux sur ce sujet crucial, afin de réaligner la perception et le comportement de ces derniers. Bien évidemment, un certain nombre d'outils technologiques peuvent aider à aligner le comportement des utilisateurs sur la politique de sécurité (ou à en minimiser les dégâts potentiels). On peut notamment citer :

- Les outils de sécurisation du poste (comme par exemple l'outil Cisco Security Agent, permettant de protéger la machine contre les attaques même si elle n'est pas à jour en terme de correctifs de sécurité tout en faisant respecter une politique de sécurité (par exemple vis-à-vis du wifi). On peut se référer à l'article portant sur l'utilisation faite de CSA en interne chez Cisco pour un retour d'expérience pragmatique.
- Les outils de contrôle d'accès (NAC) : ils permettent de contrôler la connexion de machines n'appartenant pas à l'entreprise (PC personnels, invités...), mais également de valider l'état de santé des machines se connectant afin de prémunir l'entreprise contre un certain nombre de menaces, et de forcer le respect d'une politique de sécurité.
- Les outils permettant de filtrer l'information arrivant à l'utilisateur, et empêchant la fuite d'information : Tous les outils de sécurisation tels les outils de filtrage de contenu http, de sécurisation de la messagerie, de firewall, et les outils de prévention d'intrusion ont également un rôle à jouer dans le filtrage des communications aux utilisateurs finaux. Par exemple, la fourniture d'un portail SSL aux nomades doit s'accompagner d'un filtrage réseau et applicatif (firewall et IPS) des flux. Les outils de chiffrement, et notamment de chiffrement de la messagerie, jouent également un rôle important dans la gestion de la fuite d'information (voir l'article dédié à ce sujet).

Au final, une part d'éducation vis-à-vis des populations de l'entreprise, et une part de solutions technologiques (host IPS, NAC, IPS, Web filtering, Anti-spam...) sont nécessaires afin d'obtenir un bon niveau de sécurisation des travailleurs nomades, en permettant d'aligner le comportement des utilisateurs sur les objectifs de l'entreprise en terme de politique sécurité. Dans le cadre d'une stratégie complète de gestion des risques, le développement de métriques permettant de mesurer et de suivre cet alignement reste par ailleurs souhaitable.

Pour aller plus loin

Understanding Remote Worker Security: A Survey of User Awareness vs. Behavior

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_white_paper0900aeecd8054581d.shtml



Contactez-nous :

www.cisco.fr
0800 907 375

Siège social Mondial

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis

www.cisco.com

Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France

Cisco Systems France
11 rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France

www.cisco.fr

Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis

www.cisco.com

Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912

www.cisco.com

Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :

www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie • Corée • Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France Grèce • Hong Kong SAR Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie • Mexique • Nouvelle Zélande • Norvège • Pays-Bas • Pérou Philippines • Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine • Russie Singapour • Slovaquie • Slovénie • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe



Copyright © 2007 Cisco Systems, Inc. Tous droits réservés. CCSP, CCVP, le logo Cisco Square Bridge, Follow Me Browsing et StackWise sont des marques de Cisco Systems, Inc. ; Changing the Way We Work, Live, Play, and Learn, et iQuick Study sont des marques de service de Cisco Systems, Inc. ; et Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, le logo iQ, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, le logo Networkers, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient et TransPath sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays.

Toutes les autres marques mentionnées dans ce document ou sur le site Web appartiennent à leurs propriétaires respectifs. L'emploi du mot partenaire n'implique pas nécessairement une relation de partenariat entre Cisco et une autre société. (0502R) 205534.E_ETMG_JD_10/07