

Synthèse

Rapport annuel 2015 de Cisco sur la sécurité

Aussi dynamiques que soient les attaques d'aujourd'hui, certaines constantes demeurent :

Les cybercriminels s'efforcent d'affiner ou de développer continuellement de nouvelles techniques capables d'échapper aux mécanismes de détection et de dissimuler les activités malveillantes. Parallèlement, les acteurs de la protection, à savoir les équipes chargées de la sécurité, doivent constamment améliorer leur approche pour protéger l'entreprise et les utilisateurs contre des campagnes de plus en plus sophistiquées.

Les utilisateurs se trouvent pris entre ces deux feux. Mais aujourd'hui, ils ne sont plus seulement les cibles des attaques, mais également des complices involontaires.

Notre *rapport 2015 sur la sécurité* présente les données, les analyses et les perspectives de Cisco® Security Research et d'autres experts en sécurité de Cisco. Il aborde la lutte constante à laquelle se livrent les cyberpirates et les défenseurs, et explique pourquoi les utilisateurs deviennent les maillons les plus faibles de la chaîne de sécurité.

Sujet vaste et complexe, la cybersécurité a d'importantes répercussions sur les utilisateurs, les entreprises, les pouvoirs publics, entre autres. Notre *rapport 2015 sur la sécurité* se compose de quatre sections. À première vue, ces sections et les problèmes qu'elles abordent peuvent sembler sans rapport, mais un examen plus approfondi révélera leurs liens.

Les quatre points traités dans le *rapport annuel 2015 de Cisco sur la sécurité* :

1. Le baromètre des risques
2. L'enquête sur l'efficacité des mesures de sécurité
3. Les tendances géopolitiques et du secteur
4. Changer la vision de la cybersécurité : des utilisateurs jusqu'au conseil d'administration

Télécharger le rapport 2015 de Cisco sur la sécurité à l'adresse

www.cisco.com/go/asr2015



1. Baromètre des risques

Cette section présente le résultat de l'étude menée par Cisco sur les menaces les plus récentes, y compris les dernières tendances en matière de kits d'exploits, de spams, d'attaques, de vulnérabilités et de publicité frauduleuse. Le rôle de plus en plus important des utilisateurs dans ces attaques est également examiné. Pour dégager les tendances de l'année 2014, le département Cisco Security Research a analysé des données télémétriques recueillies dans le monde entier. Le baromètre des risques présentés dans le rapport a été réalisé par des experts en sécurité travaillant dans diverses divisions de Cisco.

2. Enquête sur l'efficacité des mesures de sécurité

Pour déterminer la perception qu'ont les professionnels de la sécurité des dispositifs de protection dans leur entreprise, Cisco a interrogé des responsables de la sécurité des systèmes d'information (RSSI) et des responsables des opérations de sécurité de 9 pays et d'entreprises d'envergures différentes sur leurs ressources et procédures de sécurité. Les résultats de cette enquête sont présentés en exclusivité dans le *rapport annuel 2015 de Cisco sur la sécurité*.

3. Tendances géopolitiques et du secteur

Dans cette section, nos experts en sécurité, géopolitique et stratégies de protection identifient les tendances géopolitiques, actuelles et nouvelles, que les entreprises, et plus particulièrement les multinationales, devraient surveiller. En ligne de mire : comment le cybercrime se développe dans des zones de faible gouvernance. Sont également abordés les derniers faits marquants concernant la souveraineté, la localisation, le cryptage et la compatibilité des données.

4. Changer la vision de la cybersécurité : des utilisateurs jusqu'au conseil d'administration

Nos experts suggèrent qu'il est temps pour les entreprises d'adopter une approche différente de la cybersécurité si elles souhaitent se protéger concrètement contre les menaces. Il faut entre autres qu'elles appliquent des mécanismes de protection plus sophistiqués avant, pendant et après les attaques, qu'elles fassent de la sécurité une priorité du conseil d'administration et qu'elles appliquent nos recommandations destinées à les aider à adopter une approche plus dynamique qui les rendra capables de mieux se préparer aux attaques et de contrer les cybercriminels de manière plus innovante.

Les sujets abordés dans le *rapport annuel 2015 de Cisco sur la sécurité* convergent vers ce seul résultat : les pirates ont de plus en plus de facilité à exploiter les failles de sécurité afin de dissimuler leurs activités malveillantes. Les utilisateurs et les équipes chargées de la sécurité font tous partie du problème. Même si de nombreux acteurs de la protection pensent que leurs processus de sécurité sont optimisés et que leurs outils sont efficaces, leur niveau de préparation est perfectible. Ce qu'il se passe sur le plan géopolitique, de la législation aux risques liés à la sécurité, peut avoir une incidence directe sur les opérations de l'entreprise et sur sa gestion de la sécurité. Tous ces facteurs pris en compte, il n'a jamais été plus essentiel pour les entreprises, quelle que soit leur taille, de comprendre que la sécurité est un problème humain, que le compromis est inévitable, et qu'il est temps d'adopter une nouvelle approche de la sécurité.



Siège social aux États-Unis
Cisco Systems Inc.
San José, Californie

Siège social en Asie-Pacifique
Cisco Systems (USA) Pte. 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 numéros de fax sont répertoriés sur le site de Cisco, à l'adresse www.cisco.com/go/offices.

Cisco et le logo Cisco sont des marques commerciales ou des marques déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour consulter la liste des marques commerciales Cisco, rendez-vous sur www.cisco.com/go/trademarks. Les autres marques commerciales mentionnées dans le présent document sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1110R)