Rapport annuel
2015 sur la sécurité

Synthèse

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.

Le *rapport annuel 2015 de Cisco 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 et les pouvoirs publics, entre autres. Le *rapport annuel 2015 de Cisco 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 de Cisco
3. Les tendances géopolitiques et du secteur
4. Changer la vision de la cybersécurité : des utilisateurs jusqu'au conseil d'administration

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. Les 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 les 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.

Principales découvertes

Voici ce que révèle notre rapport annuel 2015 sur la sécurité.

Les pirates ont de plus en plus de facilité à exploiter les failles de sécurité afin de dissimuler leurs activités malveillantes.

- En 2014, 1 % des alertes urgentes du dictionnaire CVE (Common Vulnerabilities and Exposures) ont été activement exploitées. Autrement dit, les entreprises doivent lutter en priorité contre ces vulnérabilités et appliquer rapidement des correctifs. Mais utiliser des technologies de sécurité avancées ne suffit pas. Il faut également viser l'excellence des processus.
- Depuis la mise sur la touche de Blackhole en 2013, aucun autre kit d'exploits n'est parvenu à atteindre de tels taux de réussite. Toutefois, le haut du podium n'est plus autant convoité par les créateurs de kits qu'auparavant.
- Les exploitations de failles Java ont diminué de 34 %. En effet, les mécanismes de sécurité Java s'améliorent et les cybercriminels s'orientent vers de nouveaux vecteurs d'attaque.
- Les malwares Flash peuvent désormais interagir avec JavaScript pour dissimuler les activités malveillantes, ce qui les rend beaucoup plus difficiles à détecter et à analyser.
- Le volume de spams a connu une hausse de 250 % entre janvier 2014 et novembre 2014.
- Les spams de type snowshoe, impliquant l'envoi de faibles volumes de spams depuis un large ensemble d'adresses IP pour éviter toute détection, constituent un nouveau type d'attaque.

Les utilisateurs et les équipes IT font partie malgré eux du problème de la sécurité.

- Les cybercriminels comptent sur les utilisateurs pour installer des programmes malveillants ou les aider à exploiter des vulnérabilités.
- Heartbleed, faille très dangereuse, expose OpenSSL à des risques graves. Pourtant, 56 % des versions OpenSSL ont plus de 50 mois et sont donc toujours vulnérables.
- La négligence des utilisateurs sur Internet, combinée aux campagnes ciblées des cybercriminels, expose de nombreux secteurs d'activité à de plus gros risques d'attaque de malwares web. D'après le département Cisco Security Research, les secteurs pharmaceutiques et de la chimie se sont avérés les plus exposés aux malwares web en 2014.
- Les créateurs de programmes malveillants passent par les modules complémentaires des navigateurs web pour propager les malwares et les applications indésirables. Cette approche s'avère redoutablement efficace pour les cybercriminels, car de nombreux utilisateurs vouent une confiance aveugle à ces modules ou ils les considèrent simplement comme inoffensifs.

L'*enquête sur l'efficacité des mesures de sécurité de Cisco* met en évidence des décalages dans la perception du niveau de sécurité.

- 59 % des responsables de la sécurité des systèmes d'information (RSSI) considèrent que leurs processus de sécurité sont optimisés, contre 46 % des responsables des opérations de sécurité.
- Près de 75 % des RSSI jugent leurs outils de sécurité très voire extrêmement efficaces, et un quart les considère seulement moyennement efficaces.
- 99 % des personnes interrogées au sein des entreprises ayant des mesures de sécurité sophistiquées sont tout à fait d'accord sur le fait que leurs dirigeants considèrent la sécurité comme une haute priorité.
- Moins de 50 % ont recours à des outils standard tels que les correctifs et la configuration pour empêcher les incidents.
- Les grandes et moyennes entreprises sont plus susceptibles d'adopter des approches très sophistiquées en matière de sécurité, par rapport aux autres entreprises interrogées dans le cadre de cette enquête.

Sommaire

Synthèse 2

Principales découvertes 4

Pirates vs acteurs de la protection : une lutte sans merci 6

1. Étudier et comprendre le risque 7

Exploitation de failles sur le web : pour les créateurs de kit d'exploits, être au-dessus de la mêlée ne veut pas forcément dire que vous êtes le meilleur 7

Les attaques et les vulnérabilités : Java, un vecteur d'attaque sur le déclin 8

L'archéologie des vulnérabilités : les dangers de l'obsolescence et pourquoi l'application de correctifs n'est pas la seule solution 12

Les risques par secteur : le ciblage des cybercriminels et la négligence des utilisateurs, une combinaison redoutable pour les entreprises des secteurs à haut risque 13

Actualité des spams : la technique « Snowshoe » en vogue chez les spammeurs 18

Publicités frauduleuses propagées par des modules complémentaires : des dommages minimes par utilisateur, mais de gros profits 21

2. Enquête sur l'efficacité des mesures de sécurité de Cisco 24

Enquête sur l'efficacité des mesures de sécurité de Cisco : où en sont les entreprises ? 24

3. Les tendances géopolitiques et du secteur 38

Pourquoi la cybercriminalité se développe dans les zones de faible gouvernance 38

Concilier souveraineté, localisation et cryptage des données : un problème épineux 39

L'harmonisation de la notion de confidentialité des données 40

4. Changer la vision de la cybersécurité : des utilisateurs jusqu'au conseil d'administration 42

Sécurité : savoir qui accède à votre réseau, quand et comment 42

Le futur de la cybersécurité dépend de l'engagement des conseils d'administration aujourd'hui 44

Manifeste sur la sécurité Cisco : principes fondamentaux de protection contre les attaques du monde réel 45

À propos de Cisco 46

Annexe 47

Notes 52

Pirates vs acteurs de la protection : une lutte sans merci

Professionnels de la sécurité et cybercriminels se livrent une lutte sans merci : c'est à qui sera plus malin que l'autre.

Côté protection, les entreprises semblent avoir monté d'un cran en se dotant d'outils plus sophistiqués pour empêcher les attaques et en réduire l'impact. Elles reconnaissent la nécessité d'une stratégie solide en la matière et sont confiantes quant à l'optimisation de leurs processus de sécurité. Les éditeurs sont également plus attentifs : ils recherchent et corrigent les vulnérabilités dans leurs produits, coupant l'herbe sous le pied des cybercriminels.

Mais parallèlement, ceux-ci deviennent de plus en plus inventifs. Non seulement leurs méthodes d'attaque sont plus sophistiquées, mais ils parviennent également de mieux en mieux à se dissimuler :

- Ils changent très fréquemment de tactiques et d'outils, disparaissent d'un réseau avant d'être arrêtés ou choisissent prestement une autre méthode pour y pénétrer.
- Ils conçoivent des campagnes de spam en utilisant des centaines d'adresses IP afin de contourner les produits antispam d'analyse de la réputation basés sur IP.
- Ils créent des malwares qui sont véhiculés par des outils auxquels les utilisateurs font confiance, ou qu'ils considèrent comme inoffensifs, pour infecter durablement leurs machines, à leur insu.
- Lorsque les éditeurs éliminent les failles de leurs produits, ils en trouvent d'autres à exploiter.
- Ils s'efforcent de dissimuler leur présence ou de se fondre dans le paysage de l'entreprise ciblée. La phase d'infiltration dans l'infrastructure et dans les bases de données utilisateur peut prendre des semaines, voire des mois. Et ce n'est que lorsqu'ils sont prêts qu'ils passent à l'action.

D'après la nouvelle *enquête sur l'efficacité des mesures de sécurité de Cisco* (voir page 24), les professionnels de la sécurité sont optimistes et se disent bien préparés à lutter contre les cybercriminels. Malgré tout, les pirates continuent de voler des informations, de s'enrichir grâce à des escroqueries ou de perturber les réseaux à des fins politiques. Au bout du compte, la sécurité se joue sur des probabilités : même si une entreprise bloque 99,99 % des spams, certains passeront au travers des mailles du filet. Une efficacité totale est impossible à garantir.

Lorsque ces messages ou exploits atteignent effectivement les utilisateurs, ils font d'eux les maillons faibles du réseau. Les entreprises utilisent désormais plus fréquemment des solutions bloquant les attaques sur le réseau, les malwares et les spams.

Par conséquent, les cybercriminels décident parfois d'exploiter les faiblesses des utilisateurs en leur envoyant par exemple une fausse demande de réinitialisation de mot de passe.

Les utilisateurs constituent des maillons de plus en plus faibles dans la chaîne de la sécurité, et les entreprises doivent faire des choix lors de la mise en œuvre de technologies et de politiques de sécurité. Alors que les développeurs tentent de simplifier l'utilisation des applications et des logiciels et de les rendre plus intuitifs, les entreprises créent-elles de nouvelles failles exploitables par les cybercriminels ? Les entreprises doivent-elles ignorer les utilisateurs, supposer qu'on ne peut pas compter sur eux et qu'ils ne peuvent pas apprendre, et mettre en place des contrôles de sécurité plus stricts qui ralentissent leur travail ? Doivent-elles prendre le temps de sensibiliser leurs collaborateurs sur la raison d'être des contrôles de sécurité et leur expliquer clairement le rôle essentiel qu'eux-mêmes ont à jouer ?

Comme le suggèrent les principes présentés dans le manifeste sur la sécurité Cisco en page 45, cette dernière proposition est à retenir. Les solutions technologiques permettent rarement aux utilisateurs d'être des acteurs de la mise en œuvre des mesures de sécurité. En général, elles les forcent plutôt à ignorer les outils de sécurité qui ralentissent leur travail, laissant ainsi l'entreprise un peu moins protégée. Il n'est plus question de se demander *si* un réseau sera touché un jour. Tous les réseaux le *seront* à un moment ou à un autre. Que fera l'entreprise à ce moment-là ? Et si l'équipe chargée de la sécurité savait à l'avance que le réseau serait compromis, adopterait-elle une approche différente ?

Le *rapport annuel 2015 de Cisco sur la sécurité* présente les dernières analyses du groupe Cisco Security Research. L'équipe a examiné les progrès réalisés dans le domaine de la sécurité qui permettent aux entreprises et aux utilisateurs de se protéger, ainsi que les techniques et les stratégies employées par les cybercriminels pour percer ces défenses. Le rapport présente également les principales conclusions de l'*enquête sur l'efficacité des mesures de sécurité de Cisco,* qui examine les mesures de sécurité des entreprises et la perception qu'ont les personnes interrogées de leur niveau de préparation. Sont également abordés les tendances géopolitiques, les développements mondiaux en matière de localisation des données, les atouts de contrôles d'accès sécurisé plus sophistiqués, la segmentation basée sur un accès en fonction du rôle et l'importance de parler de la cybersécurité dans les conseils d'administration.

1. Étudier et comprendre le risque

Pour réaliser ses analyses, le groupe Cisco Security Research s'est appuyé sur un vaste ensemble de données télémétriques. Nos experts travaillent sans relâche sur les menaces nouvelles, comme le trafic de programmes malveillants. Leurs analyses permettent d'avoir une indication du comportement à venir des cybercriminels et aident à détecter les menaces.

Exploitation de failles sur le web : pour les créateurs de kit d'exploits, être au-dessus de la mêlée ne veut pas forcément dire que vous êtes le meilleur

Les entreprises s'efforcent de se forger une réputation de leader dans leur secteur. Mais quand des créateurs de kits d'exploits œuvrent dans l'économie souterraine, conserver une quatrième ou une cinquième place dans le classement peut être un signe de réussite encore plus parlant d'après Cisco Security Research.

Comme le *Rapport Cisco sur la cybersécurité du 1er semestre 2014* l'indique, aucun nouveau créateur de kit d'exploits ne s'est démarqué depuis fin 2013.[1] Cette date correspond à l'arrestation de « Paunch », le créateur et distributeur présumé du très efficace Blackhole, et de la mise sur la touche de ce kit d'exploits très utilisé et très bien géré. D'après Cisco Security Research, si personne ne domine, du moins pas encore, c'est simplement qu'aucun autre kit n'est capable de s'imposer comme véritable leader technologique parmi les prétendants au titre. Une autre tendance observée : depuis l'arrestation de Paunch et le démantèlement de Blackhole, de plus en plus d'utilisateurs de kits d'exploits investissent dans des kits ultrasophistiqués, capables de se soustraire à toute détection.

En 2014, Angler, Sweet Orange et Goon sont les kits d'exploits qui ont été le plus souvent observés « in vivo » d'après nos experts. Angler est celui qui a été le plus souvent détecté sur le terrain en 2014, avec un pic fin août, pour des raisons inconnues. Cisco Security Research attribue la popularité d'Angler à la décision prise par ses créateurs de permettre la propagation de malwares sans téléchargement de fichier exécutable Windows.

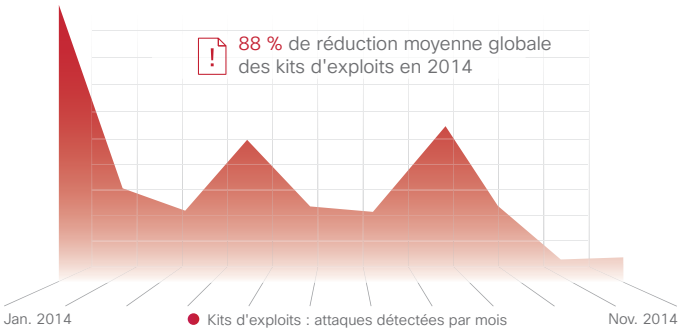
D'après nos chercheurs, l'utilisation que fait Angler des vulnérabilités Flash, Java, Microsoft Internet Explorer (IE) et même Silverlight en fait LE kit à surveiller. Une fois l'exploit déclenché, la charge utile du malware est écrite directement en mémoire dans un processus tel qu'iexplore.exe, et non pas sur un disque. La charge utile distribuée par Angler ressemble à une nuée de données cryptées, ce qui complique son identification et son blocage.

Pour en savoir plus sur Angler et comprendre l'utilisation de la publicité frauduleuse comme principal vecteur de diffusion du kit d'exploits, lisez l'article « Angling for Silverlight Exploits » publié sur le blog Cisco Security.

Le kit d'exploits Sweet Orange est lui aussi très dynamique. Ses composants, ses ports et ses URL de données utiles changent constamment : il reste donc efficace et indétectable. Cela fait de lui le kit d'exploits « le plus susceptible de réussir » d'après Cisco Security Research. Sweet Orange propage une série de programmes malveillants sur les systèmes des utilisateurs n'ayant pas appliqué les derniers correctifs et dont certains exploitent les vulnérabilités d'Adobe Flash Player, d'IE et de Java. Les cybercriminels qui utilisent Sweet Orange s'appuient souvent sur la publicité frauduleuse pour rediriger les utilisateurs vers les sites web hébergeant le kit d'exploits, y compris des sites légitimes. Les utilisateurs sont généralement redirigés au moins deux fois pendant ce processus. Autres sites propices à l'hébergement de Sweet Orange : les sites compromis qui exécutent des versions de systèmes de gestion de contenu obsolètes telles que WordPress et Joomla.[2]

Quant au kit d'exploits Goon, Cisco Security Research explique que c'est sa réputation de fiabilité qui lui a fait profiter d'une popularité modeste, mais constante en 2014. Il a également gagné le titre de kit d'exploits « le plus organisé ». D'abord découvert en 2013 par des experts en sécurité, Goon, également connu sous le nom de « Goon/Infinity », est un cadre de distribution de malwares permettant d'exploiter les vulnérabilités des composants Flash, Java ou Silverlight des navigateurs sur les plates-formes Windows et Mac.[3]

Figure 1. Tendances relatives aux kits d'exploits : nombre d'attaques détectées entre janvier et novembre 2014



Source : Cisco Security Research

La quantité globale de kits d'exploits détectés sur le terrain a chuté de 87 % dans les mois suivant la disparition de Blackhole, mais ce nombre a de nouveau augmenté en été 2014 (voir Figure 1). Dans les dernières semaines d'août, le groupe Cisco Security Research a observé un pic de détections du kit Angler. Mais en novembre, la quantité globale de kits détectés a de nouveau chuté, avec Angler et Goon/Infinity toujours en tête. La période de mai à novembre 2014 a connu un recul de 88 % en termes de détections.

Les attaques et les vulnérabilités : Java, un vecteur d'attaque sur le déclin

Ces dernières années, Java s'est retrouvé malgré lui en haut de la liste des vulnérabilités à exploiter les plus répandues et les plus graves. Mais le vent semble tourner. Java ne s'attire plus les faveurs des cybercriminels recherchant les moyens les plus rapides, les plus simples et les plus discrets d'exploiter les vulnérabilités logicielles selon Cisco Security Research.

Lisez le billet « Fiesta Exploit Pack Is No Party for Drive-By Victims » posté sur le blog Cisco Security pour découvrir comment les entreprises peuvent se protéger contre le kit d'exploits Fiesta. Ce kit propage des malwares en exploitant des vecteurs d'attaque tels que Silverlight, et il utilise les domaines DNS dynamiques (DDNS) comme pages de renvoi pour l'exploit.

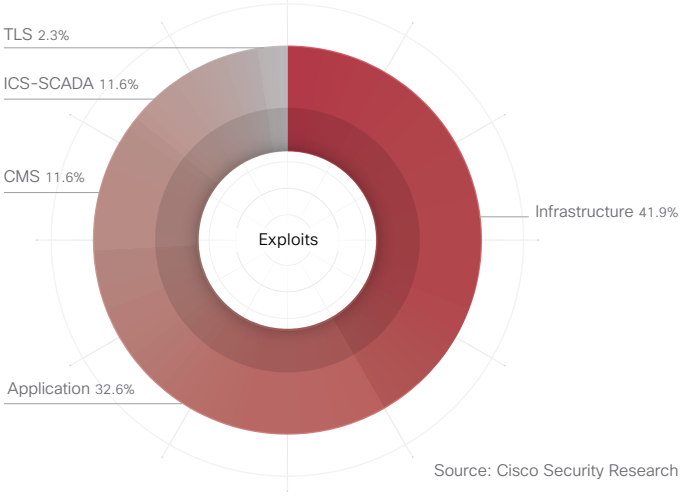
Pour en savoir plus sur le kit d'exploits Nuclear et sa capacité à évaluer le système d'un utilisateur pour en identifier les vulnérabilités et propager le type de malware approprié, consultez le billet « Evolution of the Nuclear Exploit Kit » publié sur le blog Cisco Security.

Une seule alerte Java figure dans les 25 alertes principales relatives aux vulnérabilités recensées par éditeur et par produit entre le 1er janvier 2014 et le 30 novembre 2014 (voir le Système d'évaluation standardisé de la criticité des vulnérabilités [CVSS] du Tableau 1 en page 10). En 2013, Cisco Security Research a recensé 54 nouvelles vulnérabilités Java urgentes, contre 19 en 2014. Pour autant, cela ne devrait pas empêcher les cybercriminels de s'attaquer à ces anciennes vulnérabilités qui subsistent aujourd'hui, en raison de leur popularité et de leur efficacité.

Les données du référentiel NVD (National Vulnerability Database) montrent un recul similaire : 309 vulnérabilités Java ont été recensées en 2013 et 253 nouvelles en 2014. (Cisco Security Research ne comptabilise que les vulnérabilités avec un score élevé sur l'échelle du CVSS, alors que le NVD inclut toutes les vulnérabilités détectées, ce qui explique la différence.) La Figure 2 présente les principales vulnérabilités exploitées, par éditeur et par produit en 2014.

Figure 2. Principales vulnérabilités exploitées, par éditeur et par produit

Figure 3. Principales catégories de produits exploitées



Source: Cisco Security Research

L'exploitation côté client des vulnérabilités d'Adobe Flash Player et Microsoft IE prend l'avantage sur celle des failles Java, de même que les exploits visant les serveurs (par exemple, les exploits ciblant les vulnérabilités du cadre web open source Apache Struts). Le nombre croissant d'exploits visant ce cadre est un bon exemple de la tendance actuelle : les cybercriminels compromettent les infrastructures web pour étendre leur mainmise pendant les attaques. De par sa popularité, le cadre Apache Struts constitue un point de départ logique pour les nouveaux exploits.

La Figure 3 présente les catégories de produits les visés par les exploits en 2014.

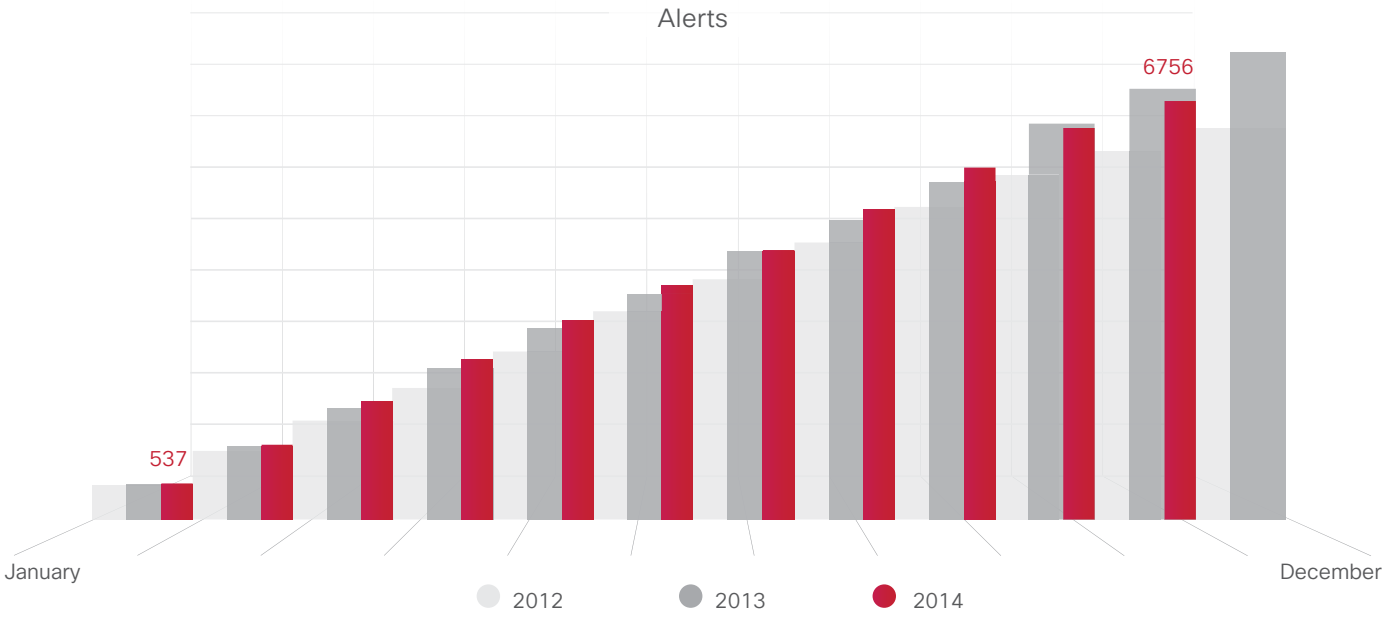
En 2014, ce sont les applications et les infrastructures qui ont été le plus fréquemment visées d'après Cisco Security Research. Les systèmes de gestion de contenu sont également des cibles privilégiées. Les pirates s'appuient sur des sites web basés sur des systèmes obsolètes pour faciliter la diffusion de l'exploit.

Baisse du nombre d'alertes annuelles cumulées

Le nombre d'alertes annuelles semble être en baisse (total cumulé des nouvelles vulnérabilités produit et des mises à jour signalées en 2014 et compilées par Cisco Security Research, voir Figure 4). En novembre 2014, cette valeur était inférieure de 1,8 % par rapport au total de 2013. Ce pourcentage peut paraître faible, mais c'est la première fois ces dernières années que le nombre d'alertes décline.

Ce phénomène s'explique certainement par l'attention grandissante portée au test et au développement des logiciels de la part des éditeurs. En effet, des cycles de vie de développement améliorés semblent réduire le nombre de vulnérabilités que les pirates peuvent facilement exploiter.

Figure 4. Nombre total d'alertes annuelles cumulées



Source: Cisco Security Research

Tableau 1. Vulnérabilités les plus souvent exploitées

Système d'évaluation standardisé de la criticité des vulnérabilités (CVSS)

ID IntelliShield	Titre	Urgence	Fiabilité	Gravité	Base	Temporalité
33695	Vulnérabilité OpenSSL TLS/DTLS Heartbeat Information Disclosure				5.0	5.0
35880	Vulnérabilité GNU Bash Environment Variable Content Processing Arbitrary Code Execution				10.0	7.4
35879	Vulnérabilité GNU Bash Environment Variable Function Definitions Processing Arbitrary Code Execution				10.0	7.4
36121	Vulnérabilité Drupal Core SQL Injection				7.5	6.2
32718	Vulnérabilité Adobe Flash Player Remote Code Execution				9.3	7.7
33961	Vulnérabilité Microsoft Internet Explorer Deleted Memory Object Code Execution				9.3	7.7
28462	Vulnérabilités Oracle Java SE Security Bypass Arbitrary Code Execution				9.3	7.7
30128	Vulnérabilité Multiple Vendor Products Struts 2 Action: Parameter Processing Command Injection				10.0	8.3

Source : Cisco Security Research

Nouvelles alertes et alertes mises à jour

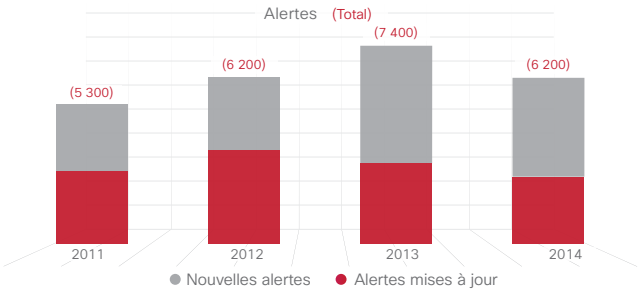
Le nombre de nouvelles alertes pour 2013 et 2014 indique que de nouvelles vulnérabilités continuent à être signalées par rapport aux années précédentes. Cela est dû au fait que les éditeurs, les développeurs et les spécialistes de la cybersécurité trouvent, corrigent et signalent davantage de nouvelles vulnérabilités dans leurs produits. La Figure 5 montre que le nombre total de nouvelles alertes et le total annuel sont stables ou en légère baisse en 2014 par rapport à 2013.

Le Tableau 1 répertorie certaines des vulnérabilités les plus souvent exploitées, selon le Système d'évaluation standardisé de la criticité des vulnérabilités (CVSS). Le référentiel NVD (National Vulnerability Database) du NIST (National Institute of Standards and Technology), une agence gouvernementale américaine, a permis de formaliser la façon de communiquer les caractéristiques et l'impact des vulnérabilités et alimente le CVSS. Dans la classification CVSS, le score « Urgence » indique que ces vulnérabilités sont activement exploitées, ce qui correspond aux scores de temporalité qui signalent des exploits actifs. Les entreprises peuvent également identifier dans la liste des produits attaqués ceux qu'elles utilisent afin de les surveiller et de les corriger.

La Figure 6 indique les éditeurs et les produits ayant obtenu les scores CVSS les plus élevés. À partir du score CVSS, Cisco indique qu'une démonstration de faisabilité existe, mais aucun code ne semble pas être disponible pour l'instant.

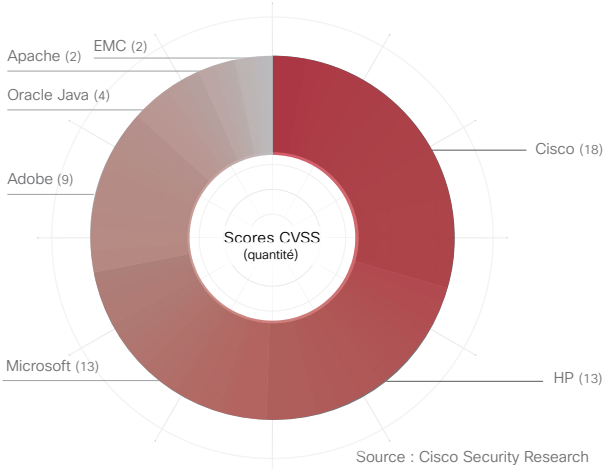
Remarque : les vulnérabilités recensées dans le Tableau 1 étaient celles qui présentaient des signes d'activité nuisible au cours de la période observée. La majorité de ces vulnérabilités n'ont pas encore été diffusées dans l'économie souterraine, c'est-à-dire qu'elles n'ont pas été intégrées dans les kits d'exploits à vendre.

Figure 5. Proportion des nouvelles alertes et des alertes mises à jour



Source : Cisco Security Research

Figure 6. Éditeurs et produits avec les scores CVSS les plus élevés



Source : Cisco Security Research

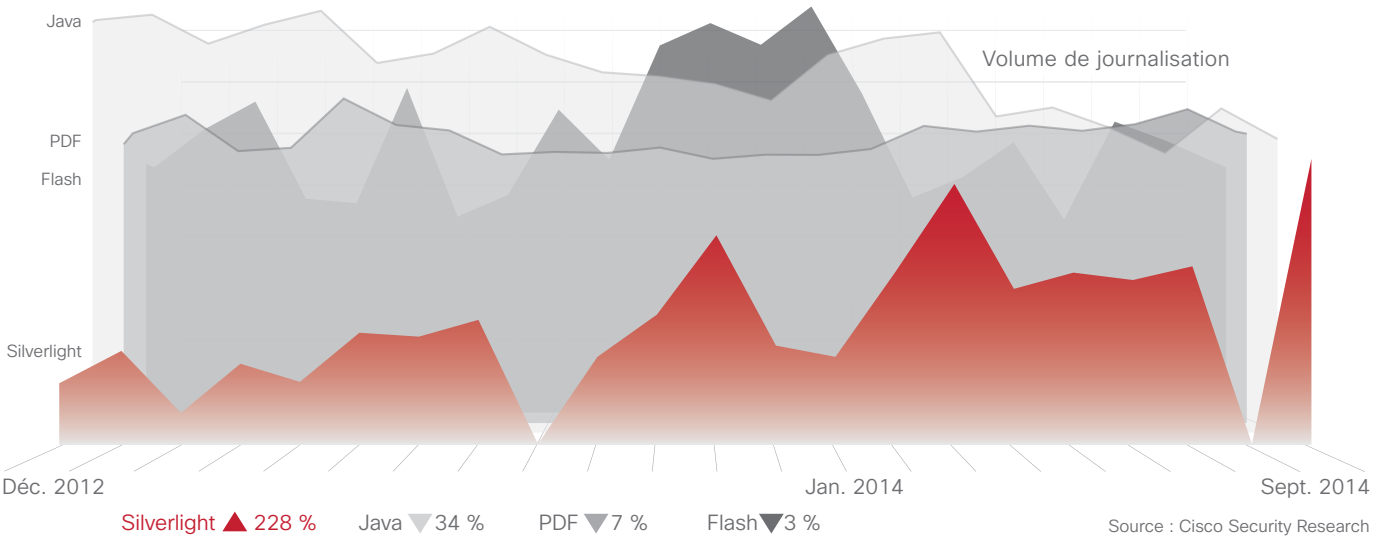
Les raisons qui ont sans doute poussé les cybercriminels à abandonner les exploits Java

L'étude réalisée par Cisco Security Research suggère que le déclin constaté des exploits Java peut en partie être dû au fait que les cybercriminels ne disposaient pas de nouveaux exploits Java de type « zero-day » en 2014. Les versions modernes de Java appliquent automatiquement des correctifs. Les versions plus anciennes et plus vulnérables de l'environnement d'exécution Java (JRE) sont, quant à elles, bloquées par défaut par les principaux éditeurs de navigateur. Apple va encore plus loin en désactivant les versions anciennes et vulnérables de Java et applique automatiquement des mises à jour de correctifs. En outre, depuis janvier 2013, l'US-CERT, le centre d'alerte et de réaction aux attaques informatiques américain, recommande aux utilisateurs de sécuriser, de désactiver ou de supprimer Java.

La dernière version de Java, Java 8, est dotée de contrôles plus performants que les versions précédentes. Cette version est également plus difficile à attaquer, car elle nécessite désormais une intervention humaine, comme la signature de code et l'activation de Java via une boîte de dialogue. Les cybercriminels ont découvert des cibles plus vulnérables et ont délaissé Java au profit de vecteurs plus rentables. Par exemple, de nombreux utilisateurs ne mettent pas à jour régulièrement leurs logiciels de lecture Adobe Flash et PDF ou leurs navigateurs. Les cybercriminels ont donc à leur disposition de nouvelles vulnérabilités à exploiter. Par ailleurs, le *rapport Cisco sur la cybersécurité du premier semestre 2014* indique que les kits d'exploits comprenant des exploits Microsoft Silverlight sont en hausse.[4]

La Figure 7 montre que la prédominance de Java en tant que principal vecteur d'attaque ne cesse de décliner depuis plus d'un an. L'utilisation de Flash pour lancer des exploits s'est montrée plutôt erratique, avec un pic au mois de janvier 2014. L'utilisation de fichiers PDF demeure constante. De nombreux pirates semblent privilégier les campagnes très ciblées de diffusion de pièces jointes PDF par e-mail. Les attaques Silverlight, bien que peu nombreuses par rapport à d'autres vecteurs plus établis, sont en hausse, surtout depuis le mois d'août.

Figure 7. Comparaison des tendances en volume par vecteur d'attaque



Flash et JavaScript : une association plus dangereuse ?

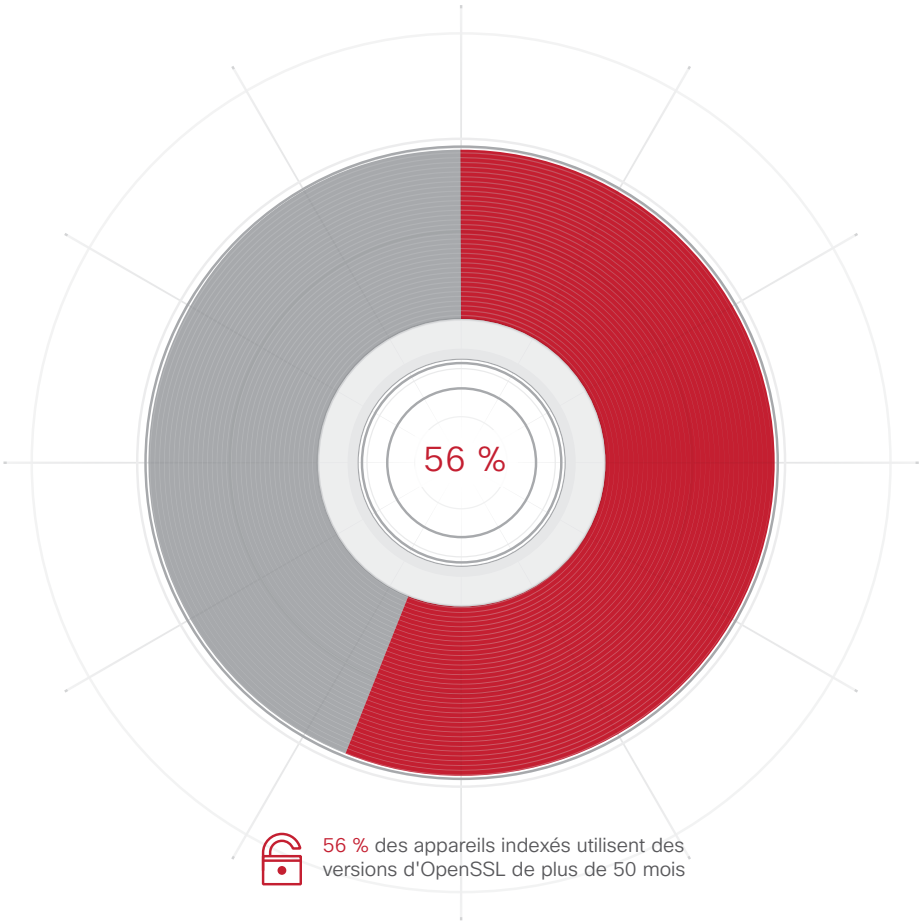
En 2014, Cisco Security Research a constaté une augmentation de l'utilisation de malwares Flash qui interagissent avec JavaScript. Ces exploits sont partagés entre deux fichiers différents, un Flash, un JavaScript. L'utilisation de deux formats de fichiers complique le travail des dispositifs de sécurité qui ont plus de difficulté à identifier, à bloquer et à analyser avec des outils d'ingénierie inverse ces « exploits partagés ». Cette approche permet également aux cybercriminels de lancer des attaques plus efficaces. Par exemple, si la première phase d'une attaque se déroule entièrement dans JavaScript, la seconde phase, soit la transmission de la charge utile, ne se produit qu'après l'exécution du fichier JavaScript. Ainsi, seuls les utilisateurs qui peuvent exécuter le malware reçoivent la charge utile.

L'archéologie des vulnérabilités : les dangers de l'obsolescence et pourquoi l'application de correctifs n'est pas la seule solution

Comme nous l'évoquons dans la section consacrée aux vulnérabilités (voir la page 8), lorsqu'ils fomentent leur attaque, les cybercriminels choisissent la voie de contamination la plus facile. Ils jettent leur dévolu sur des produits qui offrent la plus grande surface d'exposition, en général des logiciels obsolètes ou non corrigés. Par exemple, l'application de correctifs aux appliances reste problématique, car de nombreux systèmes sont toujours vulnérables aux attaques Poodle exploitant le protocole SSL.[5] À partir des tendances observées, l'étude de Cisco Security Research suggère que la prolifération des versions obsolètes de logiciels exploitables continuera à poser des problèmes de sécurité de grande ampleur.

Cisco Security Research a utilisé des moteurs d'analyse pour examiner les appareils connectés à Internet et utilisant OpenSSL. L'équipe a déterminé que 56 % des appareils examinés utilisaient des versions d'OpenSSL datant de plus de 50 mois. Ainsi, malgré toute la médiatisation dont a fait l'objet Heartbleed,[6] malgré la découverte en 2014 de la faille de sécurité dans le traitement du protocole TLS (Transport Layer Security), et malgré l'urgence d'une mise à niveau d'OpenSSL, les entreprises ne vérifient pas qu'elles exécutent les dernières versions du logiciel. La Figure 8 montre l'âge des versions d'OpenSSL.

Figure 8. Âge des versions d'OpenSSL



Source : Cisco Security Research

Solutions possibles : mises à jour et application de correctifs automatiques

Un plus grand recours aux mises à jour automatiques peut être une solution au problème des logiciels obsolètes. Les experts de Cisco Security Research ont examiné les données concernant les appareils connectés en ligne et qui utilisent le navigateur Chrome ou IE. Pour Chrome, 64 % des requêtes sont émises à partir de la version la plus récente du navigateur. Pour IE, elles ne sont que 10 %.

Selon Cisco Security Research, le système de mise à niveau automatique de Chrome semble plus efficace dans la mesure où il permet au plus grand nombre d'utilisateurs de disposer de la dernière version de ce logiciel. (Il est également possible que les utilisateurs de Chrome aient des compétences techniques supérieures à celles des utilisateurs d'IE. Ils sont ainsi plus susceptibles d'actualiser leur navigateur et d'installer les mises à jour.)

Illustrant la baisse des vulnérabilités et des exploits Java, la recherche montre clairement que les logiciels qui installent automatiquement leurs propres mises à jour présentent l'avantage de créer un cadre de sécurité plus sûr. Pour éviter la compromission pouvant résulter des mises à niveau manuelles, les entreprises doivent désormais accepter les risques d'erreur et d'incompatibilité que présentent les mises à jour automatiques.

Les risques par secteur : le ciblage des cybercriminels et la négligence des utilisateurs, une combinaison redoutable pour les entreprises des secteurs à haut risque

Le secteur pharmaceutique et de la chimie est celui qui a enregistré le plus de détections d'attaques par malwares web en 2014. Pendant le premier semestre, le secteur de la presse et de l'édition tenait le haut du pavé, mais il a reculé d'une place en novembre. Les secteurs manufacturier, des transports et de l'aéronautique complètent ce classement des 5 secteurs les plus touchés au premier semestre 2014.

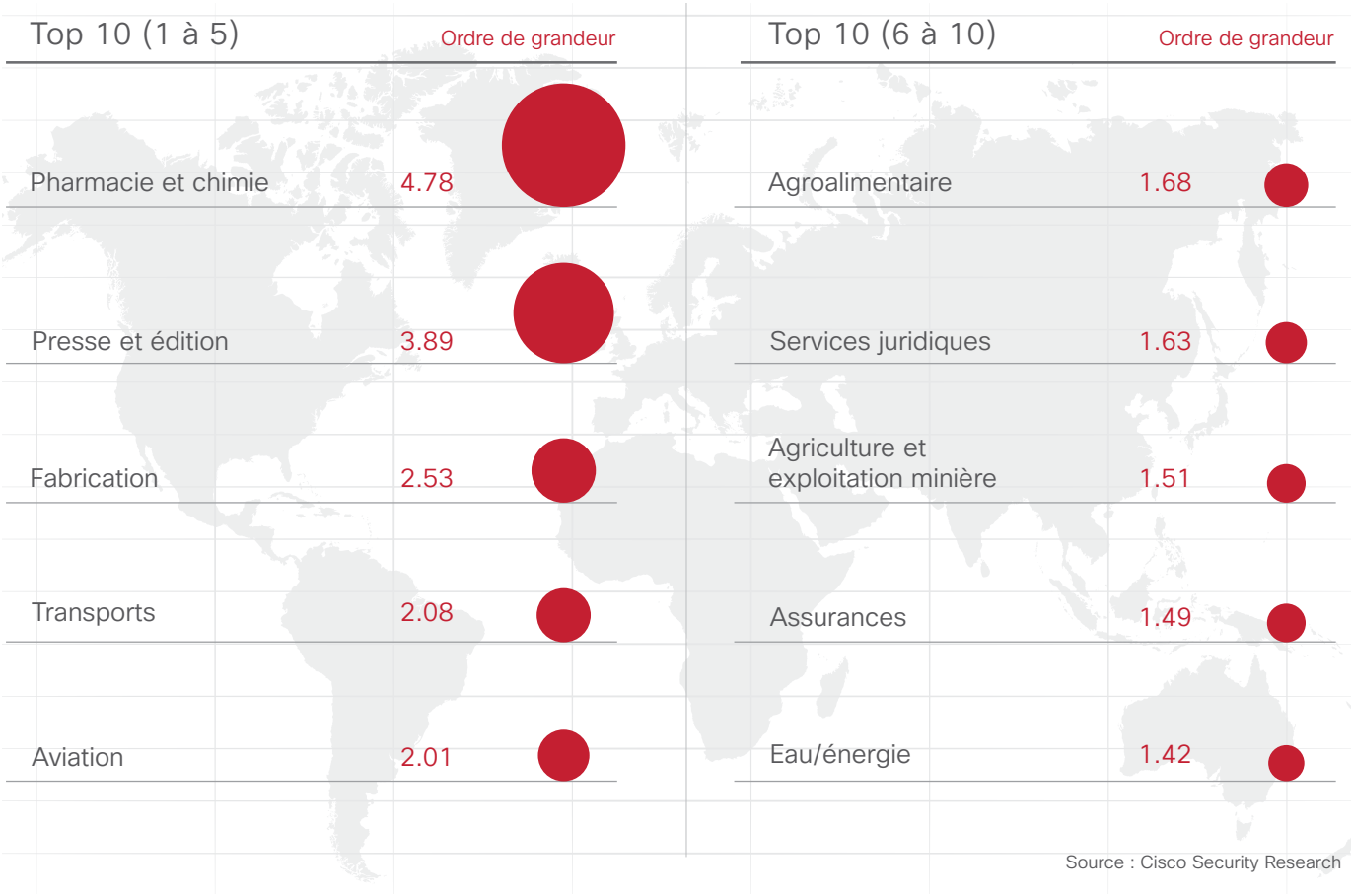
On pourrait s'attendre à ce que le secteur du commerce ait une position plus haute dans le classement étant donné les attaques sophistiquées récentes dont il a été victime. Mais le classement est établi à partir des détections d'attaques par malwares et à partir des violations de sécurité.

Pour déterminer la fréquence des détections de programmes malveillants propres à un secteur, les chercheurs de Cisco Security Research comparent le taux de fréquence moyen pour toutes les entreprises qui passent par le service Cisco Cloud Web Security au taux de fréquence médian pour toutes les entreprises d'un secteur donné qui passent par le service (Figure 9). Un taux supérieur à 1 pour un secteur témoigne d'un risque supérieur à la normale de rencontre de programmes malveillants transmis sur Internet, tandis qu'un taux inférieur à 1 indique un risque moindre. Par exemple, une entreprise qui présente un taux de 1,7 est exposée à 70 % de risques de plus par rapport à la valeur médiane. Inversement, une entreprise avec un taux de 0,7 est exposée à 30 % de risques de moins par rapport à la valeur médiane.

Détection et compromission

Une « détection », ou « rencontre », correspond au blocage d'un programme malveillant. Contrairement à une « compromission », le système de l'utilisateur n'est pas infecté lors d'une détection, car aucun fichier binaire n'est téléchargé.

Figure 9. Risque sectoriel de rencontre de malware transmis par Internet, toutes zones confondues, 1er janvier – 15 novembre 2014



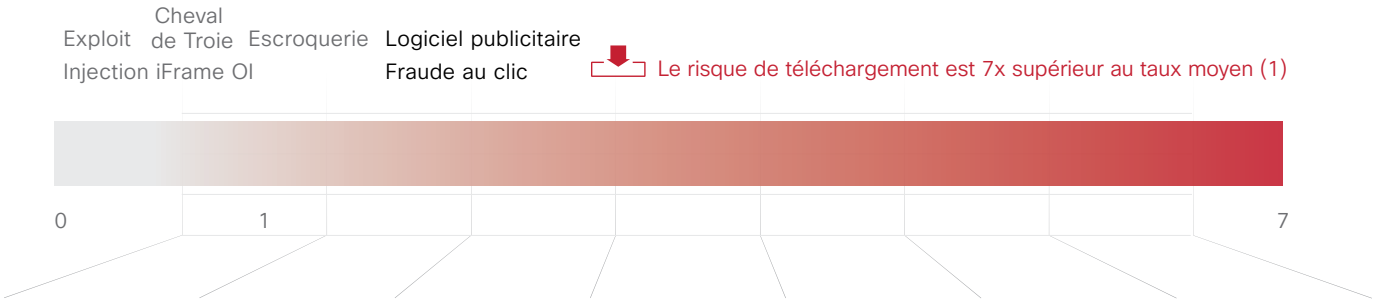
Source : Cisco Security Research

Les experts de Cisco Security Research ont étudié 8 méthodes d'attaque (Figure 10) pour déterminer si l'augmentation des détections d'attaque par malwares dans les divers secteurs d'activité était due aux cibles choisies par les cybercriminels ou au comportement des internautes. Il s'agit en fait d'une combinaison des deux. Les méthodes d'attaque ciblée et l'imprudence des internautes ont un impact sur le niveau de risque.

Pour déterminer s'il existe une différence entre un comportement présentant un risque élevé ou faible de la part des utilisateurs par secteur d'activité, les experts ont examiné quatre méthodes d'attaque non ciblée courantes : logiciels publicitaires, fraude au clic, escroquerie et injections de balises iframe. L'équipe a également examiné quatre méthodes d'attaque plus sophistiquées que les cybercriminels emploient souvent dans les campagnes ciblées : exploit, Cheval de Troie, OI (détection de programme malveillant) et téléchargement de fichiers.

Remarque : les 8 méthodes d'attaque ont été classées par les experts de Cisco Security Research dans des catégories heuristiques.

Figure 10. Méthodes d'attaque par malware transmis sur Internet : comparaison entre les 4 secteurs les plus exposés et les 4 secteurs les moins exposés



Source : Cisco Security Research

Se basant sur les résultats pour les 4 premiers secteurs les plus exposés aux programmes malveillants et les 4 derniers, établis selon les données du service Cisco Cloud Web Security, les experts de Cisco Security Research ont ensuite pris en compte le pourcentage des incidents pour chaque méthode d'attaque et ont créé des taux moyens pour ces secteurs d'activité. La comparaison illustrée dans la Figure 10 a été obtenue en divisant la moyenne supérieure par la moyenne inférieure. Un taux de 1 indique que les mêmes tendances d'activité sont observées entre les groupes les plus ciblés et les moins ciblés.

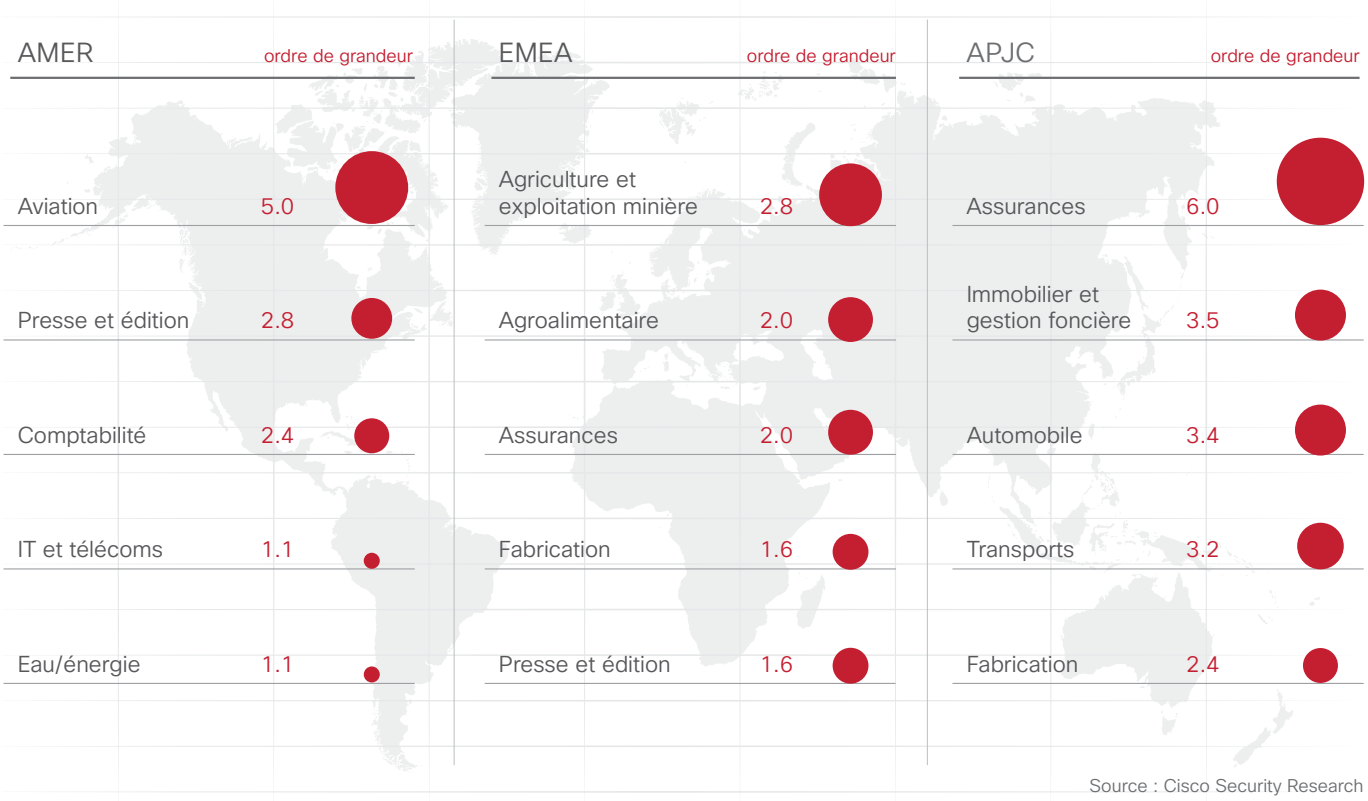
Les données montrent que les secteurs d'activité les plus exposés aux risques sont la cible d'attaques sophistiquées par le biais du téléchargement de fichiers à une fréquence sept fois supérieure par rapport aux quatre derniers secteurs de la liste. Cela est cohérent avec les résultats pour les méthodes d'attaques ciblées contre les secteurs les plus exposés aux risques.

Le taux de détection de programmes malveillants employant les fraudes au clic et les logiciels publicitaires est également plus élevé pour les secteurs les plus exposés aux risques et les plus ciblés que pour les moins exposés et les moins ciblés. Cela suggère que la différence peut être plus complexe à analyser que pour les attaques ciblées par les cybercriminels. Le comportement des utilisateurs peut également jouer un rôle dans l'augmentation des expositions aux programmes malveillants en fonction de la manière dont ils interagissent avec Internet et de leurs habitudes de navigation. Cela contribue également à la fréquence plus élevée de détection des différentes méthodes d'attaque par des programmes malveillants dans les secteurs d'activité les plus exposés aux risques. Par ailleurs, les utilisateurs dans les secteurs où l'adoption de nouveaux supports est encouragée et nécessaire pour l'innovation et la compétition sont plus susceptibles d'être exposés à des attaques par des programmes malveillants sur le web que les utilisateurs dans d'autres secteurs d'activité, notamment l'administration, où l'utilisation d'Internet peut être plus limitée, voire strictement contrôlée.

Par exemple, comme le montre l'étude de Cisco Security Research, les utilisateurs dans le secteur de la presse et de l'édition sont plus exposés à des exploits web que les utilisateurs d'autres secteurs, car ils surfent généralement plus sur d'Internet.

Remarque : en 2014, le secteur de la presse et de l'édition a enregistré des taux de détection de malwares plus élevés que ce qu'avaient précédemment observé les chercheurs de Cisco Security Research depuis 2008. L'exposition des utilisateurs à des publicités frauduleuses plus largement diffusées sur des sites web grand public peut avoir contribué à cette augmentation.

Figure 11. Secteurs d'activité les plus exposés aux attaques par malware pour les zones AMER, APJC et EMEA



Source : Cisco Security Research

Détections de programmes malveillants par zone

Nous avons répertorié les risques de rencontre de malwares transmis par Internet pour les secteurs les plus exposés par région. Les trois zones sont définies de la façon suivante :

- Amérique du Nord, Amérique centrale et Amérique latine (AMER)
- Asie-Pacifique, Chine, Japon et Inde (APJC)
- Afrique, Europe et Moyen-Orient (EMEA)

L'équipe de Cisco Security Research a identifié les secteurs d'activité les plus exposés (voir les secteurs d'activité répertoriés à la Figure 11) dans le monde et a déterminé que :

- Les utilisateurs dans le secteur de l'assurance dans la zone APJC sont 6 fois plus susceptibles d'être exposés à des malwares que dans les 12 secteurs d'activité examinés dans les trois régions. (Moyenne de base : 1,5.)
- Les utilisateurs dans le secteur aéronautique dans la zone AMER sont 5 fois plus susceptibles d'être exposés aux programmes malveillants que les autres.
- Les utilisateurs dans le secteur de l'immobilier et de la gestion foncière, ainsi que les utilisateurs du secteur de l'automobile dans la région APJC sont 3,5 fois plus susceptibles d'être exposés à des programmes malveillants que les autres.
- Les utilisateurs dans le secteur des transports dans la zone APJC sont 3,25 fois plus susceptibles d'être exposés à des programmes malveillants que les autres.

Selon Cisco Security Research, l'explosion des prix de l'immobilier et du foncier, les catastrophes naturelles récentes et la forte activité manufacturière et d'exportation dans la zone APJC expliqueraient pourquoi les attaques ciblent les utilisateurs qui travaillent ou ont des liens dans les secteurs automobile, de l'assurance, de l'immobilier et de la gestion foncière ainsi que des transports. Les vols de données des clients, de propriété intellectuelle (notamment du fait d'états) et de données de fret aérien sont probablement les principales motivations pour cibler les utilisateurs du secteur aéronautique dans la région AMER.

Méthodes de diffusion des malwares, par zone

Les Figures 12a à 12c révèlent, par zone, les techniques privilégiées par les cybercriminels pour propager des malwares. Les résultats représentés ici sont principalement basés sur les données de détection d'attaques de malwares issues du service Cisco Cloud Web Security, plutôt que sur les types de menace présents sur Internet.

Au cours de l'année 2014, les utilisateurs de la zone AMER étaient principalement ciblés par des scripts malveillants ; les attaques par injection de balises iframe venaient loin derrière. Dans la zone APJC, les cybercriminels ont eu recours à des escroqueries, des scripts malveillants et l'exploitation de failles sur Internet au cours de l'année passée pour tromper les utilisateurs dans tous les secteurs d'activité. Dans la zone EMEA, l'exploitation de failles sur Internet est particulièrement courante.

Lisez le billet « Threat Spotlight: Group 72 » publié sur le blog Cisco Security pour savoir comment l'équipe de Cisco Security Research a contribué à identifier et à mettre fin aux activités d'un groupe de cybercriminels ciblant les entreprises de premier plan qui disposent d'une propriété intellectuelle précieuse dans les secteurs manufacturier, industriel et aéronautique ainsi que de la défense et de la presse.

Pour plus de détails sur l'outil d'administration à distance RAT (Remote Administration Tool) que Group 72 a utilisé pour ses activités de cyberespionnage, lisez l'article « Threat Spotlight: Group 72, Opening the ZxShell ».

Figure 12a. Méthodes de diffusion, zone AMER

Méthode d'attaque	% total
Script	24,93 %
Injection iFrame	17,43 %
Exploit	13,63 %
OI (programme malveillant de détection)	10,35 %
Cheval de Troie	10,06 %

Source : Cisco Security Research

Figure 12b. Méthodes de diffusion, zone APJC

Méthode d'attaque	% total
Escroquerie	25,26 %
Script	25,04 %
Injection iFrame	18,68 %
OI (programme malveillant de détection)	9,93 %
Exploit	6,72 %

Source : Cisco Security Research

Figure 12c. Méthodes de diffusion, zone EMEA

Méthode d'attaque	% total
Injection iFrame	51,48 %
Script	15,17 %
Exploit	8,64 %
Escroquerie	7,31 %
OI (programme malveillant de détection)	4,16 %

Source : Cisco Security Research

Figure 13. Le nombre d'expéditeurs de spams Snowshoe est en hausse

Source : Cisco Security Research

Actualité des spams : la technique « Snowshoe » en vogue chez les spammeurs

L'hameçonnage demeure l'outil de choix des cybercriminels pour diffuser des malwares et voler des informations d'identification, car les utilisateurs continuent à tomber dans le piège des spams. Les cyberpirates ont constaté qu'il était souvent plus facile de tromper les utilisateurs par le biais de leur navigateur et de leur messagerie que d'infecter des serveurs. Les spammeurs continuent d'innover.

Il n'est pas rare de voir un système antispam bloquer plus de 99 % des spams. La plupart des meilleurs systèmes antispam en bloquent plus de 99,9 %. Mais les spammeurs font tout ce qu'ils peuvent pour éviter les filtres de spam. Ainsi, pour être sûrs d'atteindre leur cible, les spammeurs font preuve d'une ingéniosité grandissante pour échapper aux mécanismes de blocage qui reposent sur l'évaluation de la réputation des adresses IP.

Et c'est là que la technique « Snowshoe » entre en scène : Snowshoe, qui signifie « raquette », porte bien son nom. Tout comme des raquettes permettent à un randonneur de marcher sur la neige sans s'enfoncer en répartissant son poids sur une plus grande surface, la technique Snowshoe consiste à envoyer en masse des mails non sollicités à l'aide d'un grand nombre d'adresses IP, chaque adresse IP envoyant un faible volume de messages, afin d'empêcher les systèmes antispam d'enfouir ces messages. La Figure 13 montre la progression des spams de type Snowshoe entre 2013 et 2014.

Dans une récente campagne Snowshoe observée par l'équipe Cisco Security Research, les spammeurs se sont livrés à un blitz. La campagne n'a pas duré plus de trois heures, mais à un moment donné elle a atteint 10 % du trafic total de spams (Figure 14).

Pour en savoir plus sur le spam Snowshoe, lisez le billet « Spam Snowshoe Attack Comes and Goes in a Flurry » publié sur le blog Cisco Security.

Les messages Snowshoe examinés par les experts Cisco présentent des caractéristiques communes. Par exemple, leurs lignes d'objet contiennent des fautes de frappe, comme « fcature 2921411.pdf » et un nombre généré de façon aléatoire. Leurs pièces jointes sont en général des fichiers PDF contenant un Cheval de Troie exploitant une vulnérabilité dans Adobe Reader.

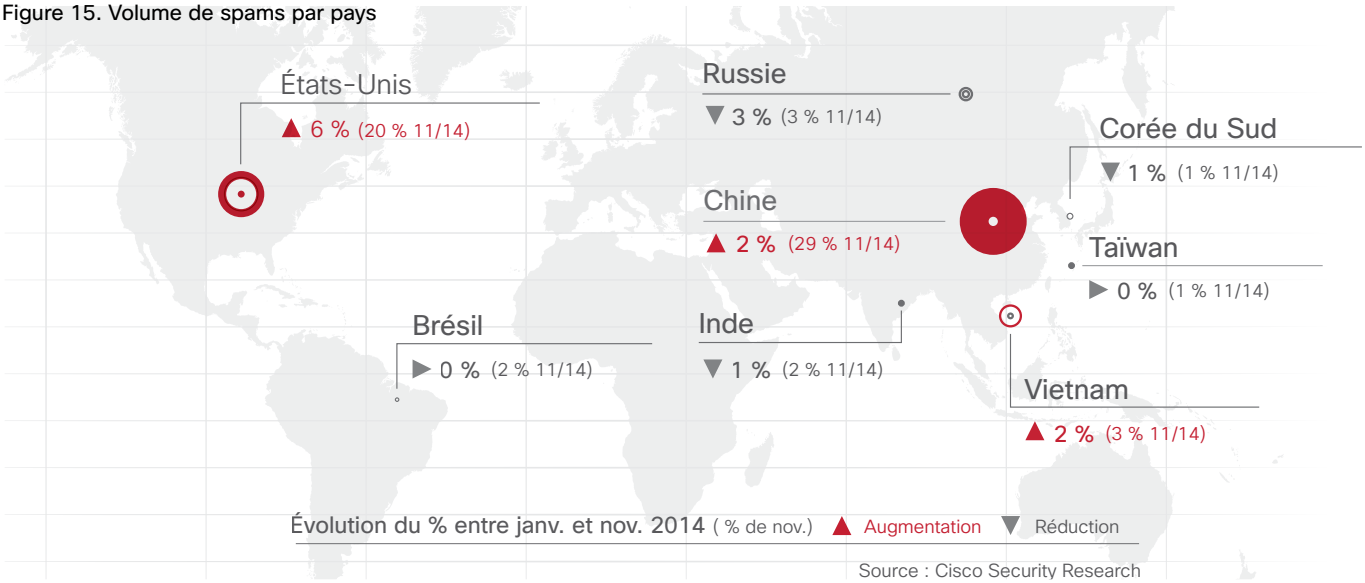
Figure 14. Campagne d'envoi de spams Snowshoe

Source : Cisco Security Research

Pour réduire la propagation de spams Snowshoe, les professionnels de la sécurité ne peuvent pas seulement compter sur des solutions d'évaluation de la réputation, car les mêmes messages dans une campagne peuvent provenir de centaines, voire de milliers d'endroits, comme c'est le cas avec les campagnes de type botnet. L'examen d'autres caractéristiques des spams, notamment l'hygiène des serveurs de messagerie, peut permettre une détection plus précise. Par exemple, dans les campagnes observées par l'équipe de Cisco Security Research, de nombreuses adresses IP étaient dépourvues de systèmes de noms de domaines (DNS) « Forward » et « Reverse », ce qui est en général le signe qu'un serveur de messagerie est illégal.

Enfin, beaucoup de ces adresses IP n'avaient aucun antécédent d'envoi d'e-mails avant le début de la campagne Snowshoe, ce qui indique également que des cybercriminels utilisent des machines compromises pour créer l'infrastructure nécessaire à l'envoi de tels spams.

Figure 15. Volume de spams par pays



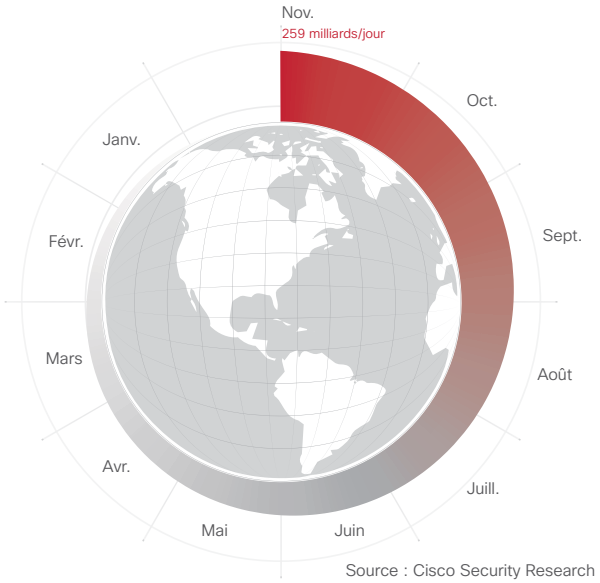
Source : Cisco Security Research

Les spammeurs diversifient leurs techniques de supercherie

Le volume de spams est en hausse, ce qui prouve qu'il s'agit toujours d'un vecteur lucratif pour les cybercriminels (Figure 16). Ces derniers peaufinent leurs messages pour tromper les destinataires et les inciter à cliquer sur des liens dangereux. Ils utilisent souvent des techniques d'ingénierie sociale.

Alors que le volume de spams a globalement baissé aux États-Unis en 2014, il a augmenté dans d'autres pays sur la même période (Figure 15). D'après Cisco Security Research, cela indique que certains cybercriminels changent leur mode opératoire. La hausse du volume de spams dans certains pays peut également indiquer qu'en matière de production de spams, d'autres régions rattrapent les États-Unis, longtemps la plus grande source de spams mondiale. Au bout du compte, les États-Unis ont terminé l'année en hausse.

Figure 16. Le volume de spams dans le monde a augmenté en 2014



Source : Cisco Security Research

Les messages de harponnage (spear-phishing), la spécialité des cybercriminels pendant plusieurs années, ont évolué à un tel que point que même les utilisateurs les plus expérimentés ont du mal à détecter les faux messages parmi ceux qu'ils reçoivent. Ces messages, qui ciblent des personnes précises, sont en général très réalistes. Ils sont destinés à leur faire croire qu'ils proviennent de fournisseurs ou de prestataires connus. Il peut, par exemple, s'agir de services de livraison ou d'écoute de musique en streaming, ou de sites d'achat en ligne. Les e-mails sur lesquels figurent un logo et un nom connus, même falsifiés, ont plus de poids que les messages de spam traditionnels faisant la promotion de médicaments ou de montres. De plus, des messages peuvent inviter le destinataire à agir, par exemple, cliquer sur des liens référençant un avis concernant une commande récente ou un numéro de traçabilité d'une livraison.

L'équipe de Cisco Security Research a récemment observé un petit nombre de messages de harponnage semblant provenir de la société Apple, qui indiquaient aux destinataires qu'ils avaient téléchargé un jeu populaire pour terminal mobile iOS. L'objet de ces messages comportait, comme marque d'authenticité, un numéro de reçu généré de façon aléatoire, tout comme sur les messages légitimes de ce type. Un lien invitait les destinataires à se connecter et à changer leur mot de passe, s'ils n'avaient pas lancé le téléchargement du jeu. Ce faisant, ils étaient redirigés vers un site d'hameçonnage connu.

Les spammeurs modifient leurs messages pour échapper à la détection

Lorsque les spammeurs trouvent une formule qui marche, à savoir une formule capable de convaincre les utilisateurs de cliquer sur des liens ou d'acheter de faux produits, ils se contentent d'adapter les messages sans changer leur structure de base. Mais les messages sont suffisamment différents pour échapper aux filtres antispam, du moins pour une courte période. Le Tableau 2 présente le nombre de tentatives de modification du contenu des messages que les spammeurs ont effectuées pour passer au travers des mesures antispam recensé par Cisco. Le tableau indique les attaques qui ont nécessité de modifier les règles de l'appliance de sécurité de la messagerie Cisco (ESA).

Tableau 2. Alertes d'attaques par spam et par hameçonnage les plus persistantes

ID IntelliShield	Titre	Version	Urgence	Fiabilité	Gravité
24986	Threat Outbreak Alert: Fake FedEx Shipment Notification	95			
31819	Threat Outbreak Alert: Fake Fax Message Delivery Email	88			
30527	Threat Outbreak Alert: Malicious Personal Pictures Attachment	81			
36121	Threat Outbreak Alert: Fake Electronic Payment Canceled	80			
23517	Threat Outbreak Alert: Fake Product Order Email Message	79			
23517	Threat Outbreak Alert: Fake Invoice Statement Attachment	78			
27077	Threat Outbreak Alert: Fake Money Transfer Notification	78			
26690	Threat Outbreak Alert: Fake Bank Payment Transfer Notification	78			

Source : Cisco Security Research

Publicités frauduleuses propagées par des modules complémentaires : des dommages minimes par utilisateur, mais de gros profits

L'équipe de Cisco Security Research a récemment étudié en détail une cyberattaque qui utilise des publicités frauduleuses propagées par le biais de modules complémentaires de navigateurs web, pour diffuser des malwares et des applications indésirables. L'équipe a découvert que le comportement de cette cyberattaque présentait de fortes similitudes avec celui des botnets. Au cours de ses recherches, qui ont notamment porté sur l'analyse de l'activité de plus de 800 000 utilisateurs dans 70 entreprises du 1er janvier au 30 novembre 2014, l'équipe de Cisco Security Research a mesuré la taille globale de l'attaque et a corroboré les similitudes avec un botnet en termes de structure et d'objectif.

L'analyse a révélé que cette famille de modules complémentaires de navigateur était bien plus diverse que prévue. L'équipe de Cisco Security Research a constaté que le stratagème avait été conçu par des professionnels qui utilisaient une combinaison de code très sophistiqué et un modèle commercial performant pour que le programme malveillant soit rentable le plus longtemps possible. En d'autres termes, prendre le contrôle de l'hôte ciblé n'est pas nécessaire pour générer des gains substantiels. Cela explique l'augmentation du nombre de malwares délibérément conçus pour avoir un impact minimal sur l'hôte infecté, mais optimisés pour garantir des gains à long terme sur le plus d'hôtes possibles.

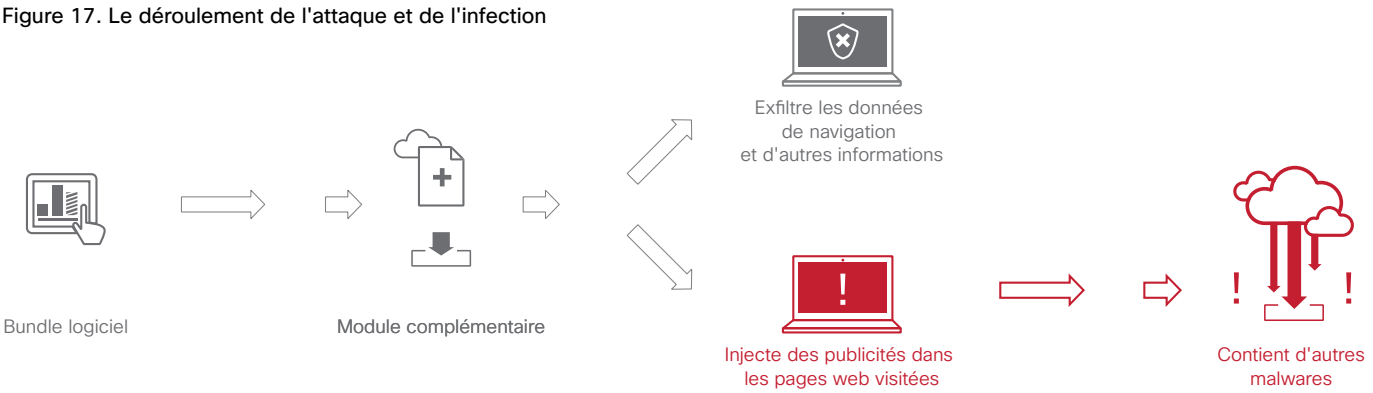
Les systèmes victimes de ces attaques sont infectés lors de l'installation d'un bundle de logiciels (un logiciel fourni avec un autre package de logiciels ou un produit) et en général sans l'accord explicite de l'utilisateur. Des applications telles que les outils PDF ou les lecteurs vidéo téléchargés depuis des sites non fiables sont installées en toute confiance par les utilisateurs qui pensent qu'il s'agit d'applications approuvées alors qu'en réalité, elles portent un logiciel malveillant et indésirable. Cette technique de diffusion de malwares repose sur un modèle de monétisation basé sur le principe du paiement à l'installation, selon lequel le créateur d'un programme malveillant est payé pour chaque installation de ce programme inclus avec l'application demandée.

La plupart des utilisateurs ont confiance dans ces modules complémentaires ou considèrent qu'ils sont peu dangereux, c'est pourquoi cette technique est considérée comme très rentable par les cybercriminels. En outre, elle leur permet d'abandonner d'autres techniques, comme les kits d'exploit, qui peuvent être plus faciles à détecter. (Voir « Exploitation de failles sur le web : pour les créateurs de kit d'exploits, être au-dessus de la mêlée ne veut pas forcément dire que vous êtes le meilleur », page 7.)

Cisco Security Research a observé que le trafic web généré par cette famille de modules complémentaires de navigateur avait des caractéristiques spécifiques et qu'il était identifiable grâce à deux modes d'action bien définis. La chaîne de requête contient en général des données codées, dans lesquelles des informations telles que le nom du module complémentaire et l'URL visitée précédemment par l'utilisateur (y compris les liens intranet) sont exfiltrées.

Au cours de l'analyse, les experts Cisco ont découvert plus de 4 000 noms de modules complémentaires, notamment PassShow, Bettersurf, Bettermarkit et les SHA associés (bee4b83970ffa8346f0e791be92555702154348c14bd8 a1048abaf5b3ca049e35167317272539fa0dece3ac1a60 10c7a936be8cbf70c09e547e0973ef21718e5). Comme plusieurs noms de module complémentaire peuvent être utilisés par installation, le malware est très difficile à détecter (Figure 17).

Figure 17. Le déroulement de l'attaque et de l'infection

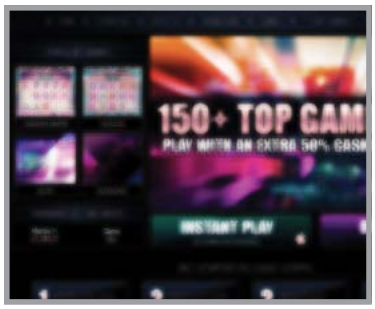


Source : Cisco Security Research

Les malwares détectent le type de système d'exploitation et passent à l'attaque

Les experts de la cybersécurité Cisco ont constaté que les modules complémentaires qu'ils ont analysés affichent un certain type de publicité en fonction de l'« empreinte » du navigateur de l'utilisateur. Les publicités injectées sur les systèmes Linux concernent en général des sites de jeux en ligne. Les utilisateurs de Microsoft IE sont redirigés vers des publicités qui déclenchent le téléchargement de logiciels apparemment fiables, mais qui sont en réalité malveillants.

Linux

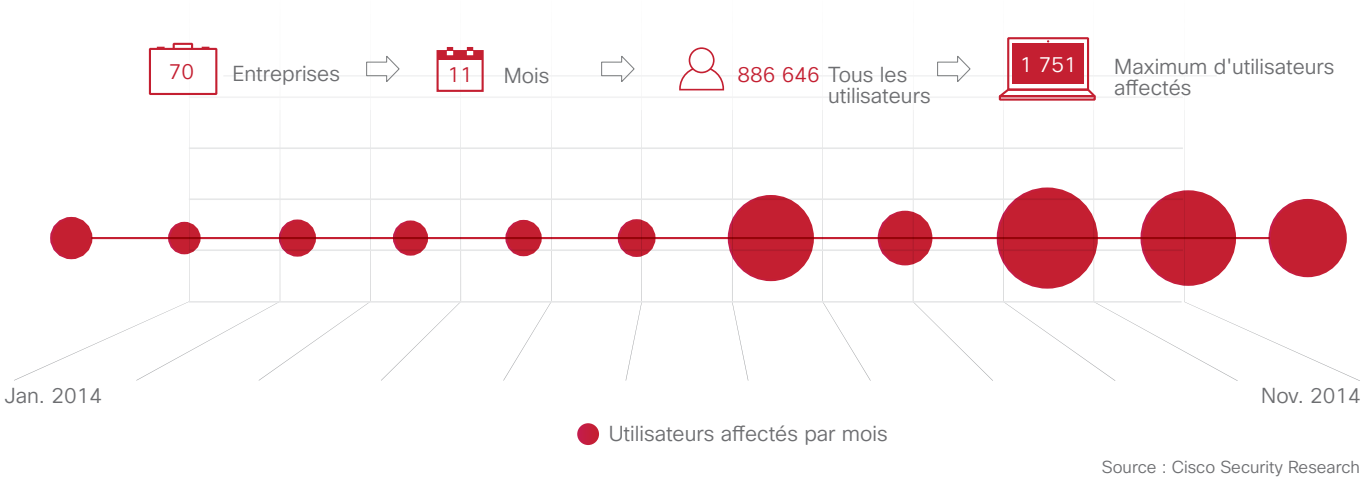


Microsoft IE

Selon l'analyse du comportement des utilisateurs de 70 entreprises réalisée sur une période de 11 mois, le nombre de victimes de cette attaque est en hausse. En janvier, 711 systèmes étaient infectés, mais dans la seconde moitié de l'année, ils étaient plus de 1 000, avec un pic de 1 751 systèmes en septembre (Figure 18). La hausse importante en septembre et octobre peut s'expliquer par une recrudescence de l'activité en ligne due au retour des vacances d'été.

Les experts de la cybersécurité Cisco ont découvert que les cybercriminels employaient plusieurs serveurs pour lancer leurs attaques. Cela signifie qu'un groupe de cybercriminels passé maître dans l'art de segmenter ses activités est probablement responsable de l'attaque, mais il peut aussi s'agir d'un « fournisseur de technologie » qui vend ses produits à plusieurs groupes. Quoi qu'il en soit, la personne à l'origine de la diffusion du malware semble avoir pour but de créer un botnet de taille conséquente.

Figure 18. Nombre de systèmes infectés par mois, de janvier à novembre 2014



Source : Cisco Security Research

Partager le rapport

Les experts de Cisco Security Research ont découvert plus de 500 domaines uniques associés à cette attaque ; 24 d'entre eux sont classés sur Alexa parmi le million de domaines les plus utilisés. De nombreux autres domaines occupent une place assez élevée dans le classement (Figure 19). Il s'agit donc de domaines populaires mais très dangereux pour les utilisateurs en raison du risque de compromission.

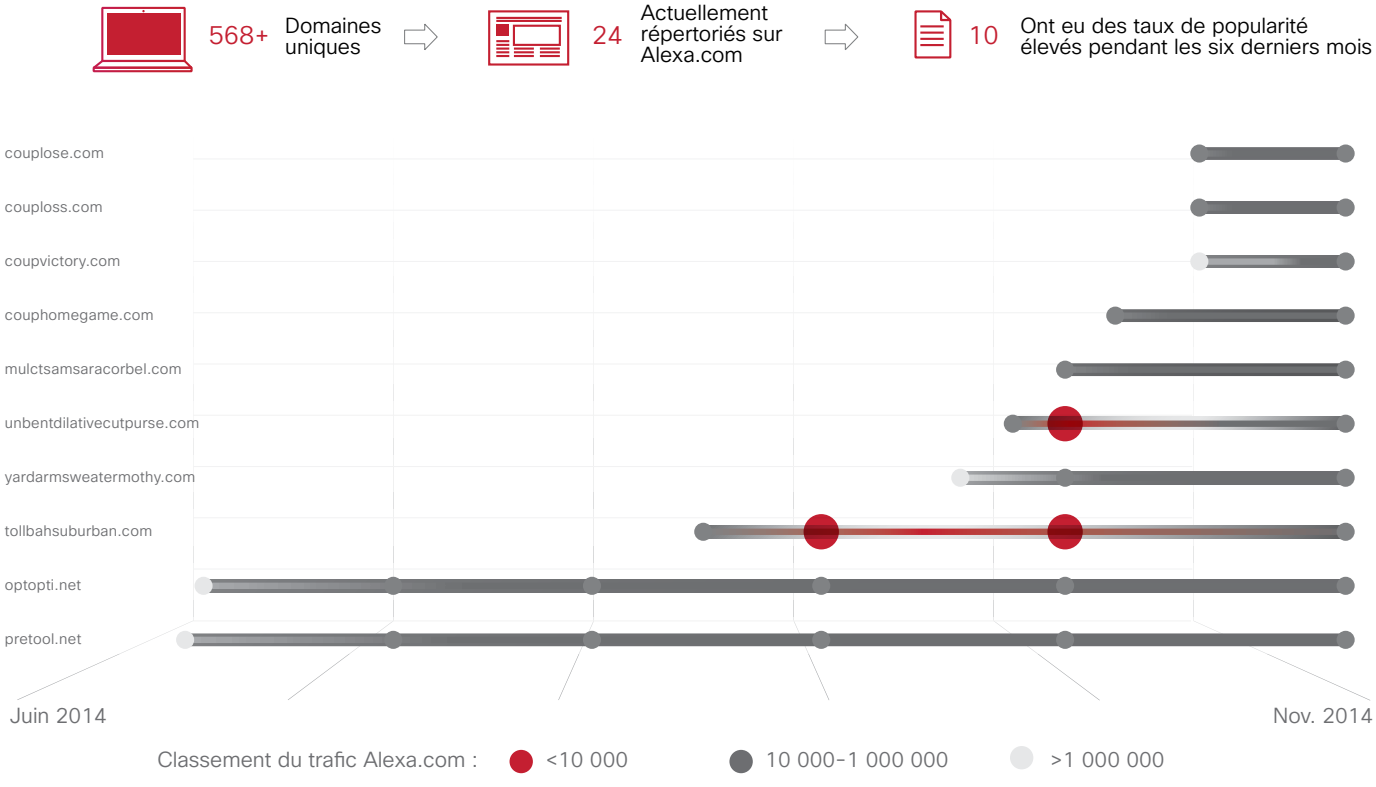
Certains domaines sont actifs depuis plus d'un an, mais d'autres ont un cycle de vie beaucoup plus court, de quelques semaines seulement dans de nombreux cas (Figure 19). Tous les domaines ont une caractéristique en commun : ils deviennent populaires très rapidement.

Conseils de prévention et de résolution

Pour éviter d'être infecté par le biais des modules complémentaires de navigateur ou pour éliminer une infection, il est conseillé aux utilisateurs de :

- Télécharger des applications uniquement depuis des sources fiables
- Désélectionner les logiciels indésirables dans les bundles d'installation
- Recourir à des solutions d'analyse des menaces ainsi qu'à des technologies de sandboxing et de protection du web pour détecter et contrer ce type d'attaque
- Supprimer manuellement les modules complémentaires, si possible et utiliser des outils antimouchards pour supprimer les programmes indésirables

Figure 19. Domaines populaires servant à héberger les publicités frauduleuses dans les attaques par modules complémentaires, classés sur Alexa



Source : Cisco Security Research

Partager le rapport

2. Enquête sur l'efficacité des mesures de sécurité de Cisco

Pour savoir comment les professionnels de la sécurité perçoivent les mesures adoptées par leur entreprise en la matière, Cisco a interrogé des responsables de la sécurité des systèmes d'information (RSSI) et des responsables des opérations de sécurité (SecOps) d'entreprises de différentes tailles, dans plusieurs pays, sur leurs ressources et procédures de sécurité. L'enquête *sur l'efficacité des mesures de sécurité de Cisco*, réalisée en octobre 2014, apporte un éclairage sur le niveau de sophistication des stratégies de sécurité en vigueur dans les entreprises.

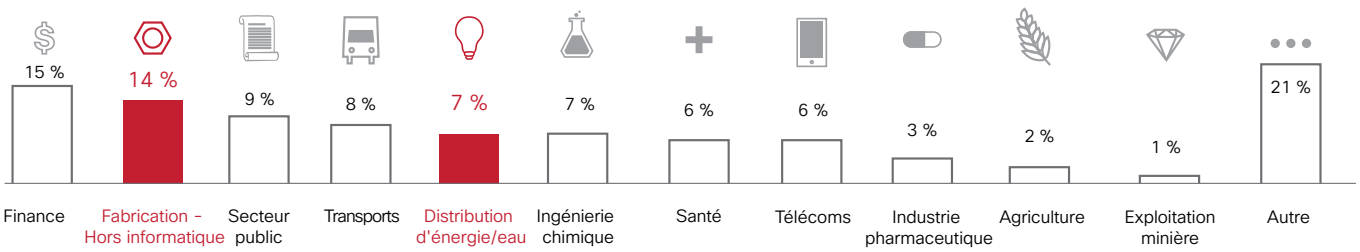
Enquête sur l'efficacité des mesures de sécurité de Cisco : où en sont les entreprises ?

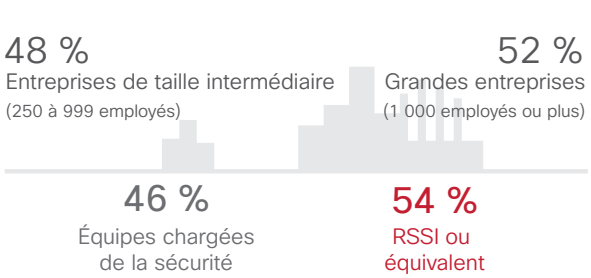
Comment les professionnels de la sécurité évaluent-ils la capacité de leur entreprise à faire face aux incidents ? La réponse dépend de leur rôle dans l'entreprise et du secteur d'activité de celle-ci, selon la nouvelle étude sur l'efficacité des mesures de sécurité réalisée par Cisco.

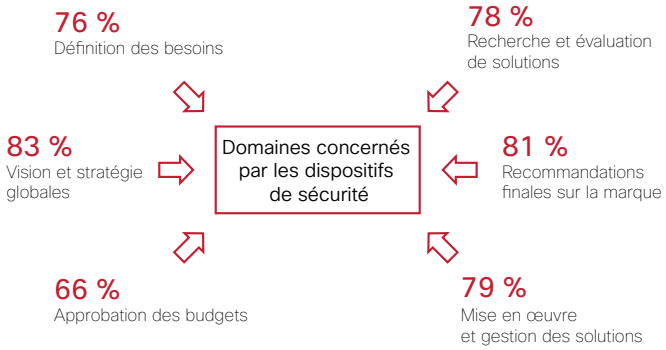
La Figure 20 montre les réponses des professionnels de la sécurité par secteur d'activité et par taille d'entreprise. Les sondés évoluant dans les secteurs de la fabrication (hors informatique), de la distribution d'énergie/eau se montrent les plus impliqués et les plus informés en matière de sécurité.

N (nombre de personnes interrogées) = 1 738

Figure 20. Profil des personnes interrogées et niveau de préparation en matière de sécurité







Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Partager le rapport

L'étude menée auprès de responsables de la sécurité des systèmes d'information (RSSI) et de responsables des opérations de sécurité (SecOps) visait à en savoir plus sur les ressources consacrées par leur entreprise à la cybersécurité, aux opérations de sécurité ainsi qu'aux politiques et aux procédures en la matière. Elle visait également à déterminer le niveau de perfectionnement des opérations de cybersécurité. Point positif : la majorité des professionnels de la sécurité déclarent disposer des outils et des processus nécessaires pour assurer une protection efficace. Cependant, les RSSI sont bien plus optimistes en la matière que leurs collègues des opérations de sécurité. Par exemple, 62 % d'entre eux s'accordent à dire que les processus de sécurité dans leur entreprise sont clairs et bien compris contre seulement 48 % des RSSI. Ces derniers voient également leurs processus de sécurité sous un jour plus favorable. 59 % d'entre eux pensent que leurs processus sont optimisés et qu'ils doivent simplement être perfectionnés contre 46 % des responsables des opérations de sécurité.

Pourquoi les avis diffèrent-ils ? En matière de gestion quotidienne de la sécurité, les RSSI sont moins impliqués contrairement au personnel chargé des opérations de sécurité qui doit résoudre les incidents mineurs et majeurs. Le RSSI d'une très grande entreprise ne sait peut-être pas qu'au cours d'une journée normale, un millier de machines peuvent être infectées par un malware, alors qu'un responsable des opérations de sécurité a plus travaillé à l'élimination de l'infection. Il est donc normal que ce dernier soit, comme ses homologues, moins optimiste.

En outre, les RSSI peuvent être amenés à définir des politiques, notamment pour bloquer l'accès aux réseaux sociaux, ce qui leur donne l'illusion que la protection en vigueur est plus étroite et impénétrable. Cependant, si de tels canaux sont complètement coupés, les équipes chargées de la sécurité peuvent ne pas avoir connaissance des attaques à la porte de leurs réseaux, et par conséquent ne pas les traiter.

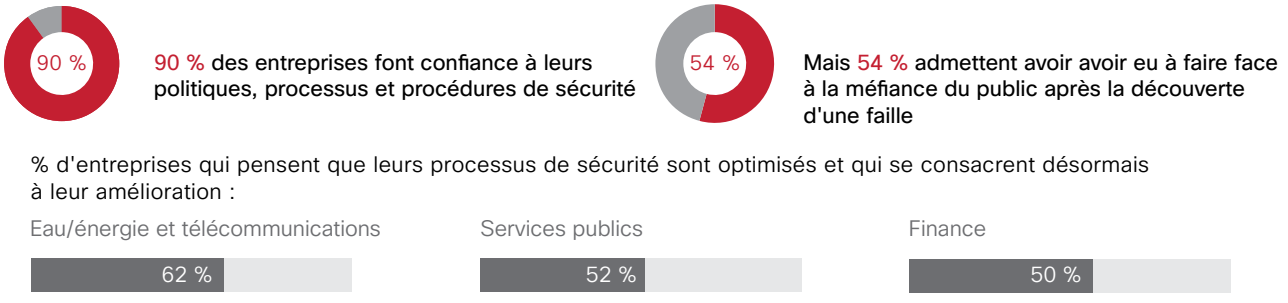
Une autre différence est apparue dans les réponses concernant la confiance dans les politiques de sécurité appliquées par les entreprises. Les RSSI et les responsables des opérations de sécurité se montrent très confiants vis-à-vis des politiques en vigueur (voir la Figure 21) ; cependant, ils le sont moins vis-à-vis de leur capacité à évaluer et à contenir les attaques (voir la Figure 28).

On constate un écart similaire entre les réponses concernant les contrôles de sécurité. Presque toutes les personnes interrogées ont indiqué que les contrôles de sécurité étaient satisfaisants, mais environ un quart d'entre elles considèrent leurs outils comme étant seulement « assez » au lieu de « très » ou « extrêmement » efficaces (voir la Figure 29).

La confiance dans les processus et les pratiques de sécurité semble également varier selon les secteurs d'activité. Les RSSI et les responsables des opérations de sécurité des entreprises du secteur de l'énergie et des services publics ainsi que du secteur des télécommunications semblent être les plus confiants contrairement à leurs homologues travaillant dans le secteur public, les services financiers, le secteur pharmaceutique et les organismes de santé. Par exemple, 62 % des responsables de la sécurité dans le secteur des télécommunications et dans celui de la distribution d'énergie/eau sont convaincus que leurs processus de sécurité sont optimisés, contre 50 % de leurs homologues travaillant dans les services financiers et 52 % dans le secteur public.

Ceux travaillant dans les secteurs de la distribution d'énergie/eau et des télécommunications semblent avoir adopté des stratégies plus perfectionnées en matière de protection, contrairement à ceux du secteur public et de la finance. Les entreprises dans le secteur de la distribution d'énergie/eau semblent disposer de procédures et de processus bien documentés pour le suivi des incidents. Pour autant, cela ne signifie forcément pas qu'elles sont mieux protégées que les entreprises des autres secteurs.

Figure 21. Principales conclusions par secteur d'activité et fonction des personnes interrogées



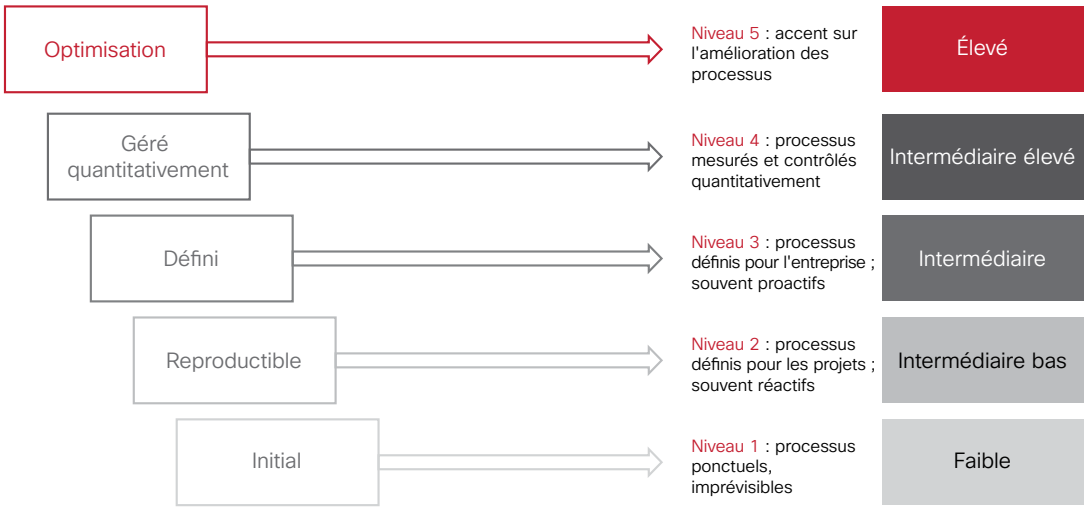
Le faible écart entre les grandes et moyennes entreprises indique que le nombre d'employés n'a aucun rapport avec le degré de sophistication des processus de sécurité.

Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Partager le rapport

Figure 22. Équivalents CMMI des niveaux de sophistication de l'échantillon étudié

Cisco a exploré plusieurs possibilités avant de s'arrêter sur 5 niveaux déterminés à partir d'une série de questions relatives aux processus de sécurité. Cette solution correspond d'assez près au modèle CMMI (Capability Maturity Model Integration).



Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Indicateurs du niveau de sophistication des mesures de sécurité

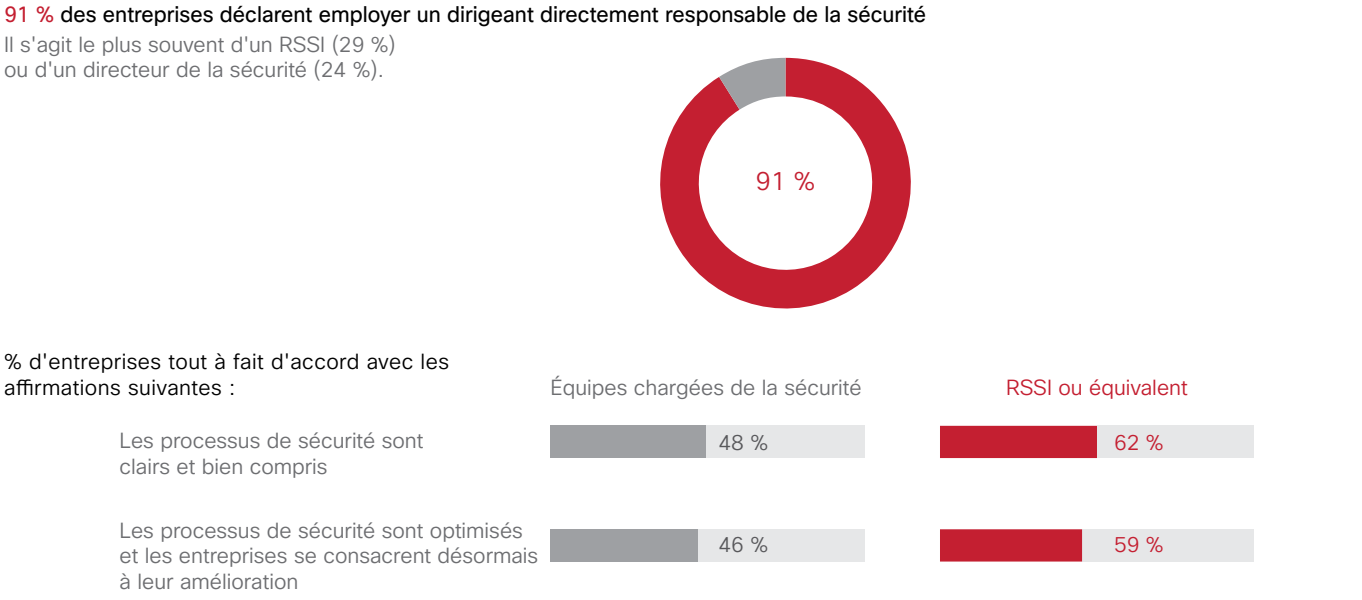
L'*étude sur l'efficacité des mesures de sécurité réalisée par Cisco* présente les caractéristiques des entreprises qui ont adopté une approche plus sophistiquée de la sécurité. Notamment, dans ces entreprises :

- La sécurité est une priorité pour les dirigeants
- Les politiques et les procédures sont claires et bien documentées
- Les outils intégrés fonctionnent ensemble

99 % des personnes interrogées dans les entreprises qui ont une approche sophistiquée s'accordent à dire que les dirigeants considèrent la sécurité comme une priorité, contre 22 % dans les entreprises avec une approche peu sophistiquée. En outre, 88 % des personnes interrogées dans les entreprises de la première catégorie déclarent que les processus de sécurité sont clairs et bien compris contre 0 % dans les entreprises de la seconde catégorie.

Partager le rapport

Figure 23. Principales conclusions sur la prise en charge des problématiques de sécurité par la direction



Les RSSI (et postes équivalents) sont plus optimistes que les responsables des opérations de sécurité quant à la sécurité dans leur entreprise, peut-être parce qu'ils sont moins en contact avec la réalité quotidienne.

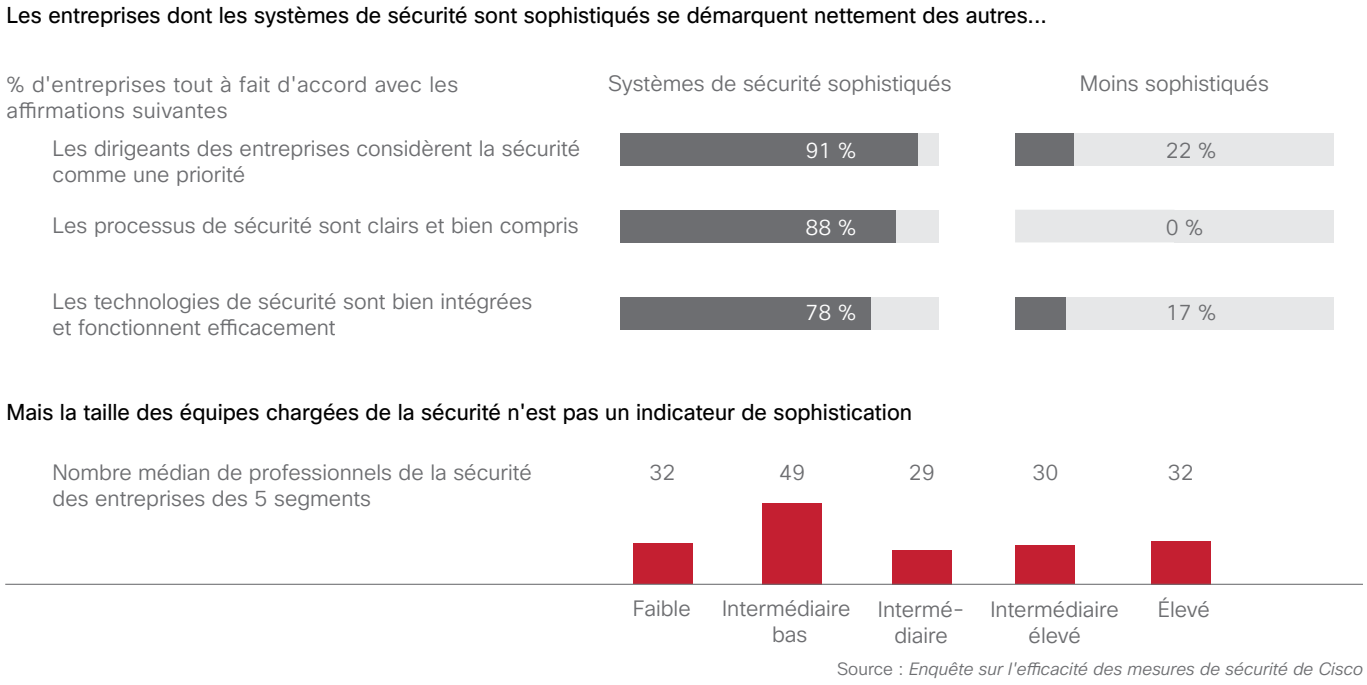
Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

La Figure 23 montre que 91 % des personnes interrogées confient que, dans leur entreprise, la responsabilité directe de la sécurité incombe à un dirigeant, généralement à un RSSI ou à un responsable de la sécurité. Les entreprises sont de plus en plus nombreuses à recruter une personne de référence en la matière. Cette tendance est encourageante : sans un tel spécialiste, les processus sont moins bien définis, partagés et appliqués. Il est fort probable que les récents incidents de grande envergure aient poussé les dirigeants des entreprises à s'intéresser à la gestion de la sécurité.

78 % des personnes interrogées représentant des entreprises ayant une stratégie sophistiquée en matière de sécurité s'accordent à dire que les technologies de protection sont bien intégrées pour fonctionner efficacement ensemble. Elles ne sont que 17 % à être de cet avis dans les entreprises où la stratégie est moins sophistiquée.

La bonne nouvelle pour les entreprises qui espèrent optimiser leurs processus de sécurité est qu'il n'est pas forcément nécessaire de créer une grande équipe d'individus talentueux difficiles à dénicher. Quel que soit le degré de sophistication, les équipes de sécurité comptent en moyenne 32 personnes. Par conséquent, il semble que la qualité de la gestion des processus de sécurité ne soit pas directement liée au nombre de professionnels de l'équipe. Il serait préférable de trouver la proportion idéale de personnel de sécurité par rapport au nombre total de collaborateurs de l'entreprise.

Figure 24. Principales conclusions sur la priorité accordée à la sécurité



Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

La Figure 24 révèle que les entreprises ayant une stratégie moins sophistiquée estiment généralement que leurs dirigeants ne considèrent pas la sécurité comme une priorité et que les processus de sécurité ne sont pas clairs ni bien compris.

En comparant le niveau de sophistication des entreprises par pays, on se rend compte d'une autre bonne chose : les entreprises qui ont adopté des mesures sophistiquées constituent la majorité de chaque segment. En revanche, dans certains pays, les personnes interrogées semblent avoir une vision plus positive de leur propre sécurité qu'elle ne l'est en réalité. Cet excès de confiance peut provenir des valeurs sociales au cœur de leur culture, par exemple le besoin de se présenter, et par extension de présenter leur entreprise, sous un jour favorable.

Attention à l'excès de confiance

Même si les RSSI et les responsables des opérations de sécurité font confiance à leurs solutions, ils déclarent également ne pas utiliser d'outils standard capables de parer les atteintes à la sécurité. Moins de 50 % des personnes interrogées ont recours aux outils suivants :

- Gestion des identités ou provisionnement des utilisateurs
- Application de correctifs et configuration
- Tests de la pénétration
- Analyse des terminaux
- Analyse des vulnérabilités

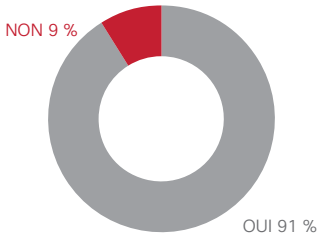
Les ressources dédiées à la sécurité dans les entreprises

Figure 25. Nombre de professionnels dédiés à la sécurité dans les entreprises

Les entreprises comptent en moyenne 123 professionnels dédiés à la sécurité. Les services publics sont le secteur le plus susceptible d'externaliser ses services de sécurité.

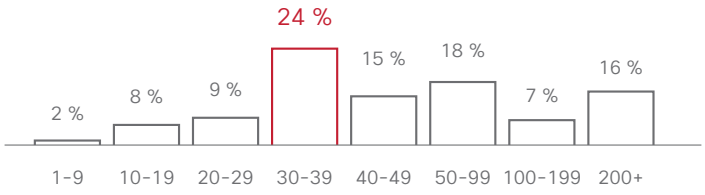
Les ressources de sécurité en bref

Votre entreprise compte-t-elle une équipe dédiée à la résolution des incidents ?



Nombre moyen de professionnels dédiés à la sécurité

Pourcentage moyen de temps consacré aux tâches relatives à la sécurité



Nombre de professionnels dédiés à la sécurité

Dans le secteur public, les services de sécurité sont davantage externalisés qu'ailleurs.

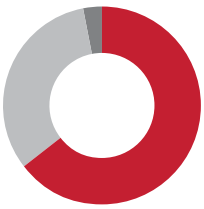
Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Figure 26. Les technologies de protection utilisées par les entreprises

Environ deux tiers des personnes interrogées affirment que leurs technologies de protection sont à jour et fréquemment actualisées.

Comment décririez-vous votre infrastructure de sécurité ?

Base : n=1 738



64 % Notre infrastructure de sécurité est à jour, nous la mettons continuellement à niveau avec les meilleures technologies disponibles.

33 % Nous remplaçons ou mettons à niveau nos technologies de sécurité régulièrement, mais nous ne possédons pas les outils les plus récents.

3 % Nous remplaçons ou mettons à niveau nos technologies de sécurité uniquement lorsque les anciennes ne fonctionnent plus ou deviennent obsolètes, ou en cas d'identification de besoins totalement nouveaux.

Une proportion sensiblement plus importante de RSSI (70 %) affirme que l'infrastructure de leur entreprise est systématiquement à jour, par rapport aux responsables des opérations de sécurité (57 %).

Les entreprises de télécommunications sont les plus susceptibles de déclarer que leur infrastructure de sécurité est maintenue à jour.

Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Figure 27. Les mesures de protection utilisées

Les diverses méthodes de protection utilisées par les entreprises en 2014.

	Mesures de protection utilisées par entreprise		Protection assurée via des services cloud	
	Équipes chargées de la sécurité n=797	RSSI n=941	Équipes chargées de la sécurité n=759	RSSI n=887
Sécurité réseau, pare-feu/prévention des intrusions	57 %	64 %	30 %	39 %
Sécurisation du web	56 %	62 %	33 %	41 %
Sécurisation de la messagerie	53 %	58 %	33 %	41 %
Prévention des pertes de données	55 %	55 %	-	-
Cryptage/confidentialité/protection des données	52 %	55 %	-	-
Autorisation/contrôle d'accès	55 %	52 %	24 %	24 %
Authentification	54 %	51 %	24 %	22 %
Mobilité sécurisée	48 %	54 %	24 %	32 %
Réseau sans fil sécurisé	47 %	52 %	22 %	30 %
Protection des terminaux/antimalwares	45 %	52 %	24 %	27 %
Analyse des vulnérabilités	44 %	51 %	24 %	26 %
VPN	49 %	46 %	25 %	27 %
Administration des identités/provisionnement des utilisateurs	43 %	47 %	16 %	23 %
Gestion des systèmes de gestion des informations et des événements de sécurité (SIEM)	39 %	46 %	-	-
Analyse des réseaux	41 %	43 %	-	-
Application de correctifs et configuration	38 %	40 %	-	-
Tests de pénétration	39 %	37 %	20 %	19 %
Protection contre les attaques par déni de service (DDoS)	35 %	37 %	-	-
Analyse des terminaux	29 %	33 %	-	-

Personnes interrogées chargées de la sécurité qui utilisent des solutions de protection ; n=1 646

13 % des personnes interrogées déclarent qu'aucune des mesures de protection utilisées n'est gérée via des services cloud. Ce résultat s'observe particulièrement dans les secteurs de la santé, de la finance et pharmaceutique

Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Figure 28. Niveaux de confiance dans les politiques de sécurité de l'entreprise et dans sa capacité à contenir les attaques

Alors que les entreprises semblent faire confiance à leurs politiques de sécurité, elles sont plus sceptiques face à leur capacité à évaluer et à contenir les attaques.

Niveaux de confiance dans les politiques de sécurité de l'entreprise

Politiques de sécurité n=1738	Équipes chargées de la sécurité n=797			RSSI n=941		
	Pas d'accord/D'accord/Tout à fait d'accord			Pas d'accord/D'accord/Tout à fait d'accord		
Les informations sont répertoriées et classées clairement	11 %	40 %	49 %	4 %	38 %	58 %
Nous gérons très bien la sécurité des RH	9 %	45 %	46 %	4 %	36 %	60 %
Les installations IT de mon entreprise sont bien protégées	10 %	39 %	51 %	4 %	34 %	62 %
Les contrôles de sécurité techniques des systèmes et des réseaux sont bien gérés	6 %	41 %	53 %	3 %	31 %	66 %
Les droits d'accès aux réseaux, aux systèmes, aux applications, aux fonctions et aux données sont contrôlés de manière appropriée	8 %	35 %	57 %	4 %	32 %	64 %
Nous intégrons efficacement les dispositifs de sécurité dans les systèmes et les applications	10 %	38 %	52 %	4 %	32 %	64 %
Nous intégrons efficacement les dispositifs de sécurité dans nos procédures d'acquisition, de développement et de maintenance des systèmes	9 %	41 %	50 %	4 %	35 %	61 %

Niveaux de confiance dans la capacité des entreprises à contenir les vulnérabilités

Opérationnalisation de la sécurité n=1738	Équipes chargées de la sécurité n=797			RSSI n=941		
	Pas d'accord/D'accord/Tout à fait d'accord			Pas d'accord/D'accord/Tout à fait d'accord		
Nous révisons et améliorons nos pratiques de sécurité de manière régulière, formelle et stratégique sur le long cours	7 %	42 %	51 %	3 %	36 %	61 %
Nous possédons des outils qui nous permettent d'examiner les mesures de sécurité en place et de donner notre avis sur ces dernières	10 %	41 %	49 %	4 %	39 %	57 %
Nous recherchons systématiquement l'origine des incidents	11 %	40 %	49 %	3 %	37 %	60 %
Nous pouvons améliorer les contrôles de sécurité sur les ressources essentielles en cas de besoin	10 %	43 %	47 %	3 %	38 %	59 %
Nous examinons régulièrement les activités de connexion sur le réseau pour nous assurer que les mesures de sécurité fonctionnent comme prévu	8 %	39 %	53 %	4 %	33 %	63 %
Nos dispositifs de détection et de blocage des attaques sont maintenus à jour	9 %	38 %	53 %	3 %	36 %	61 %
Nos technologies de sécurité sont bien intégrées et fonctionnent efficacement	9 %	40 %	51 %	3 %	37 %	60 %
La sécurité est bien intégrée avec les objectifs et les processus de notre entreprise	10 %	39 %	51 %	2 %	34 %	64 %
Il est facile de déterminer l'étendue de la menace, de l'éliminer et d'empêcher l'exploitation future de la faille	15 %	44 %	41 %	8 %	42 %	50 %

Davantage de personnes interrogées dans les PME sont tout à fait d'accord avec l'affirmation concernant « l'examen et l'amélioration des pratiques de sécurité de manière régulière, formelle et stratégique sur le long cours » par rapport aux personnes interrogées dans les grandes entreprises.

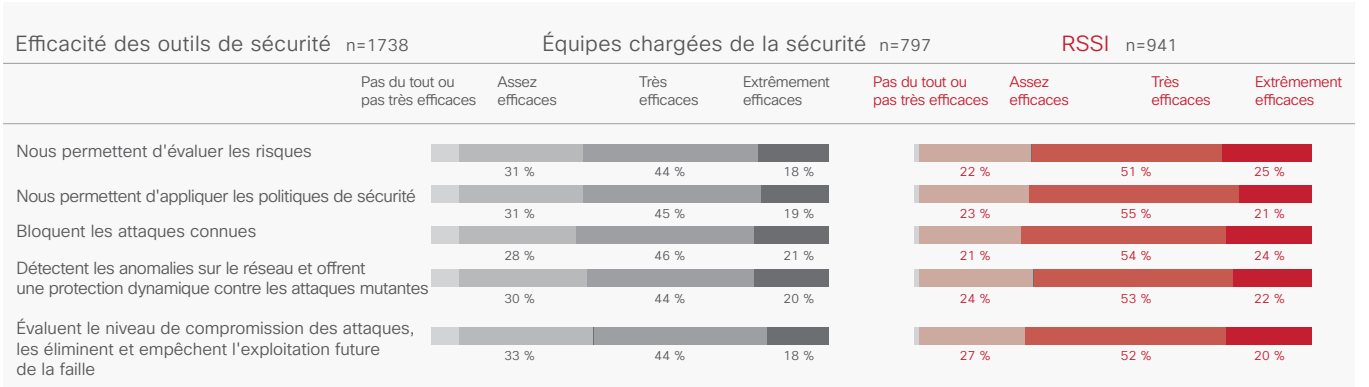
Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Figure 29. Avis des personnes interrogées sur les contrôles et les outils de sécurité de l'entreprise

Les professionnels de la sécurité estiment que leur entreprise dispose de contrôles de sécurité appropriés, mais environ un quart des personnes interrogées considèrent que leurs outils de sécurité ne sont pas vraiment efficaces.

Contrôles de sécurité n=1738	Équipes chargées de la sécurité n=797			RSSI n=941		
	Pas d'accord	D'accord	Tout à fait d'accord	Pas d'accord	D'accord	Tout à fait d'accord
Nous suivons les pratiques de résolution d'incident standard telle que la norme RFC2350, ISO/IEC 27035:2011 ou une certification américaine	15 %	42 %	43 %	6 %	40 %	54 %
Nous utilisons des processus efficaces pour interpréter, hiérarchiser et comprendre les rapports d'incident	11 %	46 %	43 %	4 %	39 %	57 %
Nous avons de bons systèmes pour vérifier que des incidents se sont produits	11 %	41 %	48 %	4 %	36 %	60 %
Nous utilisons un bon système pour classer les informations relatives aux incidents	10 %	43 %	47 %	4 %	37 %	59 %
Nous veillons à informer les parties prenantes et à collaborer avec elles	10 %	46 %	44 %	3 %	40 %	57 %
Nous avons des processus et des procédures bien documentés pour la résolution et le suivi des incidents	9 %	40 %	51 %	4 %	35 %	61 %
L'évaluation des risques liés à la cybercriminalité est systématiquement intégrée à notre processus global d'évaluation des risques	10 %	37 %	53 %	4 %	36 %	60 %

Sensiblement plus de personnes du secteur de la distribution d'énergie et d'eau ont déclaré être tout à fait d'accord avec l'affirmation Nous avons des processus et des procédures bien documentés pour la résolution et le suivi des incidents que les professionnels de la plupart des autres secteurs.



Les professionnels de la sécurité du secteur des transports sont moins confiants dans la capacité de leur entreprise à détecter les attaques connues et à s'en protéger.

Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Figure 30. Processus mis en œuvre pour analyser les systèmes compromis et pour éliminer les causes des incidents

Les professionnels de la sécurité sont plus enclins à recourir aux fichiers journaux du pare-feu pour analyser les incidents, même si ces journaux ne leur fournissent généralement pas de données pleinement exploitables, ni de contexte. Pour une meilleure analyse des failles, les professionnels de la sécurité doivent régulièrement consulter les journaux IDS et IPS, le proxy, les systèmes de prévention des intrusions basés sur les hôtes (HIPS), les journaux des applications et NetFlow.

Il est également surprenant de voir que l'« analyse de corrélation entre journaux et événements » figure si loin dans la liste des outils utilisés pour évaluer les vulnérabilités. Les personnes interrogées ne mettent peut-être pas les données ou les sources de données en corrélation, or ces méthodes permettent une analyse plus poussée des incidents.

Processus d'analyse des systèmes compromis	Équipes chargées de la sécurité	RSSI
	n=797	n=941
Fichier journal du pare-feu	59 %	62 %
Analyse du journal système	58 %	60 %
Analyse de régression des fichiers ou des malwares	51 %	58 %
Analyse des flux réseau	51 %	54 %
Analyse des registres	48 %	51 %
Analyse par capture intégrale des paquets	44 %	48 %
Analyse de corrélation entre journaux et événements	40 %	44 %
Analyse de la mémoire	39 %	43 %
Analyse des disques	38 %	41 %
Détection d'indicateurs de compromission (IOC)	38 %	38 %
Équipes externes [ou tierces] d'analyse/de résolution d'incidents	36 %	38 %

Les personnes interrogées travaillant dans le secteur public ont tendance à utiliser davantage de processus d'analyse des systèmes compromis que celles des autres secteurs.

Processus d'élimination de la cause des incidents	Équipes chargées de la sécurité	RSSI
	n=797	n=941
Mise en quarantaine ou suppression de l'application malveillante	55 %	60 %
Analyse de cause première	55 %	56 %
Arrêt de la propagation du malware	51 %	55 %
Surveillance supplémentaire	51 %	53 %
Mise à jour des politiques	50 %	51 %
Arrêt de la propagation de l'application compromise	47 %	49 %
Développement de correctifs à long terme	46 %	48 %
Restauration de l'image précédente du système	43 %	47 %

Les réponses des RSSI et des équipes chargées de la sécurité sont cohérentes, à l'exception de l'arrêt de la propagation du malware.

Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Figure 31. Réponses des RSSI et des responsables des opérations de sécurité concernant les contrôles mis en œuvre après un incident

Davantage de RSSI déclarent mettre en œuvre des contrôles supplémentaires après un incident que les responsables des opérations de sécurité.

Processus de restauration des systèmes affectés	Équipes chargées de la sécurité	RSSI
	n=797	n=941
Mise en œuvre de nouveaux contrôles et dispositifs de détection, en fonction des vulnérabilités identifiées après un incident	55 %	65 %
Application de correctifs et mise à jour des applications jugées vulnérables	59 %	60 %
Restauration à partir d'une sauvegarde préincident	53 %	60 %
Restauration différentielle	53 %	58 %
Restauration de l'image de référence	33 %	36 %

Les personnes interrogées dans le secteur des télécommunications et de la distribution d'énergie/eau déclarent utiliser la restauration de l'image de référence davantage que dans les autres secteurs.

Figure 32. À qui sont signalés les incidents ?

Le personnel chargé des opérations et les partenaires technologiques sont plus susceptibles d'être informés d'incidents par des moyens plus formels.

Groupes notifiés en cas d'incident	Équipes chargées de la sécurité	RSSI
	n=797	n=941
Opérations	44 %	48 %
Partenaires technologiques	42 %	47 %
Ingénierie	38 %	37 %
Ressources humaines	37 %	35 %
Services juridiques	37 %	35 %
Tous les employés	38 %	33 %
Fabrication	31 %	36 %
Partenaires commerciaux	31 %	33 %
Marketing	30 %	31 %
Relations publiques	30 %	27 %
Autorités externes	25 %	20 %

Les administrations publiques sont beaucoup plus susceptibles que les entreprises des autres secteurs d'avoir recours à des notification de notification clairement définis, avec plus de groupes.

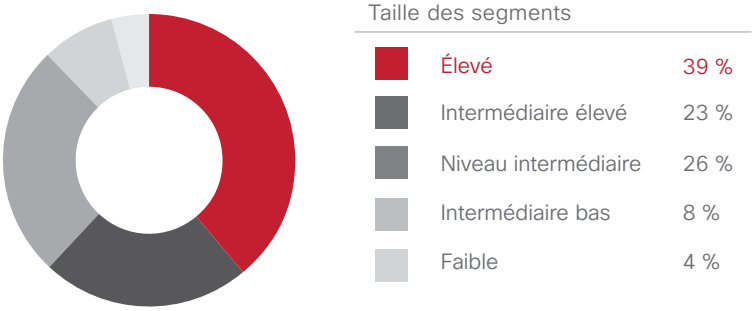
Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Niveau de sophistication de la sécurité dans l'entreprise

Figure 33. Niveau de sophistication des processus de sécurité

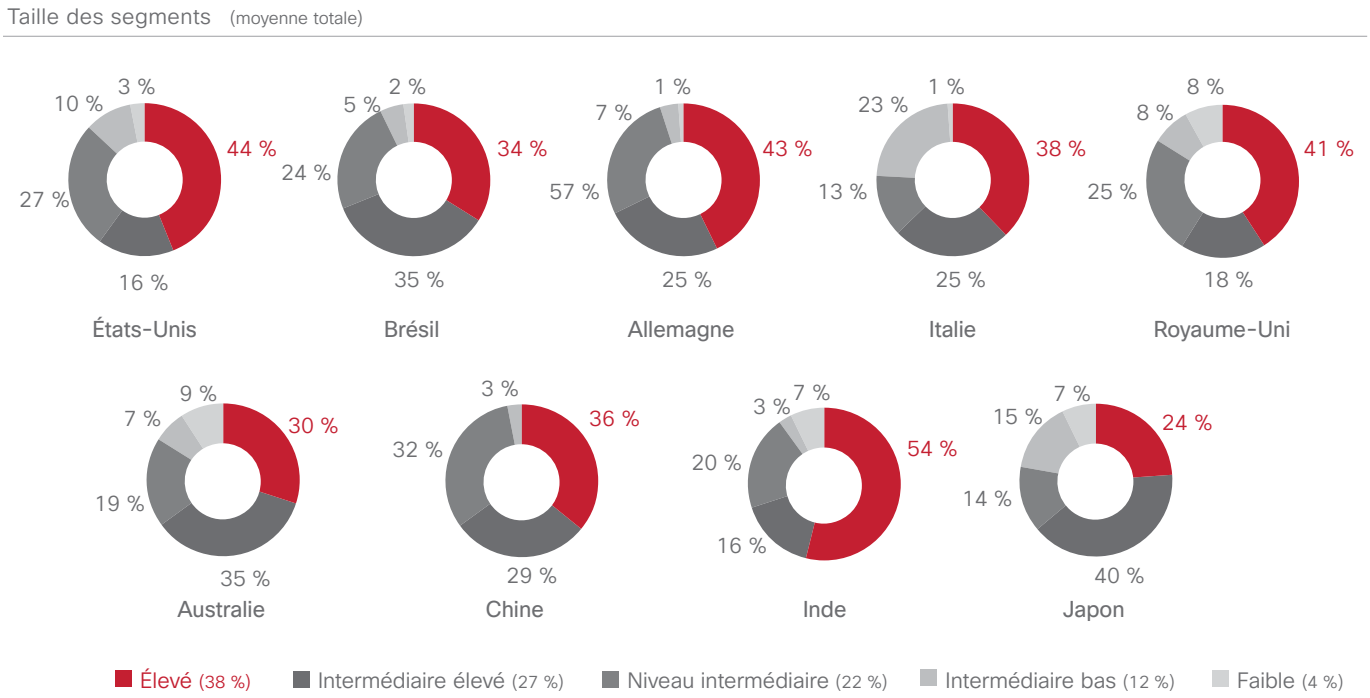
La plupart des entreprises ont des profils de sécurité plus sophistiqués, dans tous les pays (Figure 34) et dans tous les secteurs (Figure 35).

Les segments reflètent la hausse des niveaux de sophistication concernant la priorité de la sécurité et les conséquences pour les processus et les procédures



Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

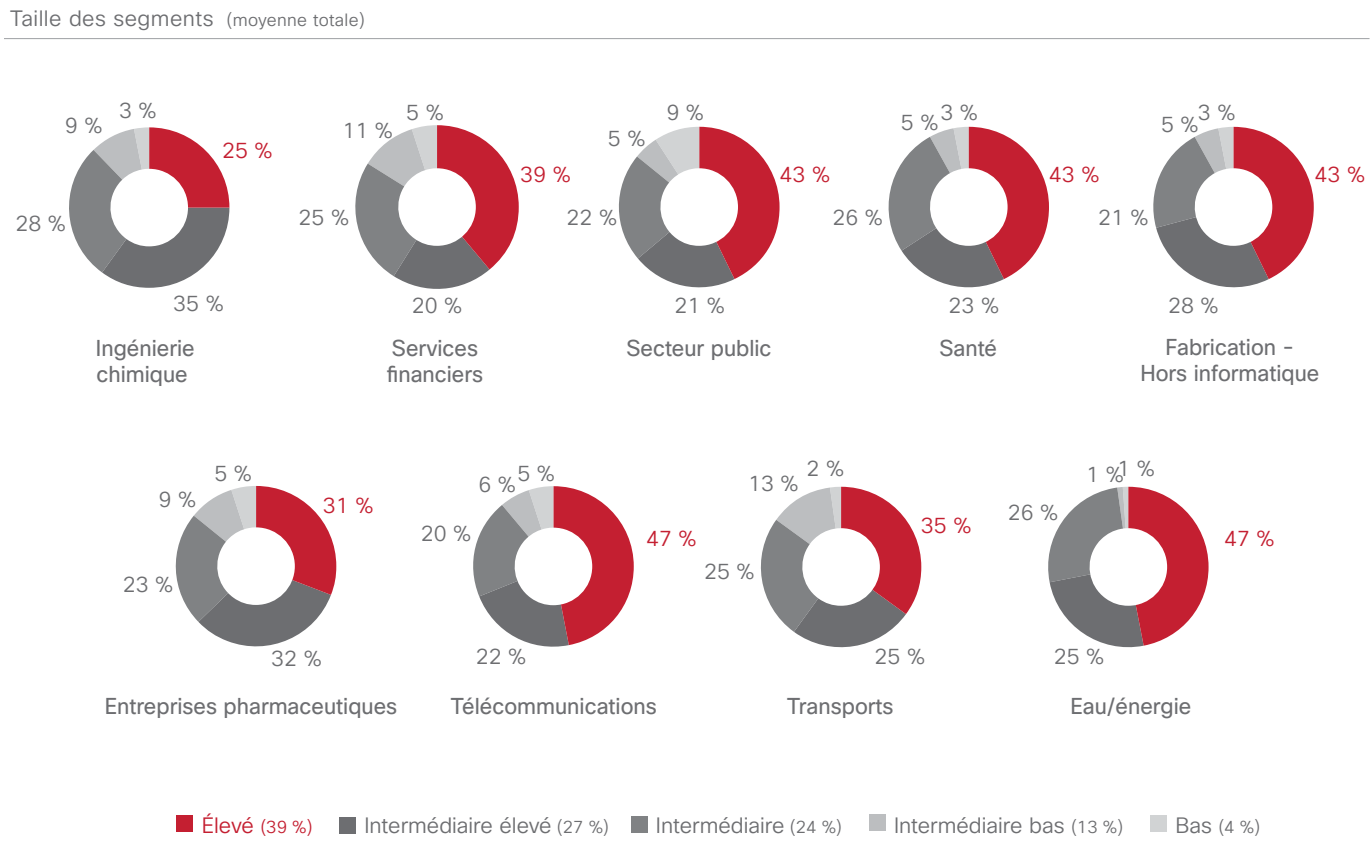
Figure 34. Niveau de sophistication des processus de sécurité par pays



Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Figure 35. Niveau de sophistication des processus de sécurité par secteur

Près de la moitié des entreprises qui œuvrent dans le secteur des télécommunications, de la distribution d'énergie et d'eau font partie du segment de sécurité le plus sophistiqué.



Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

Sécurité : la bonne préparation des PME

Sans surprise, les très grandes entreprises gèrent avec brio les questions de sécurité vu les nombreuses ressources auxquelles elles ont accès : le budget pour acheter les dernières technologies et des collaborateurs compétents pour les gérer. Les grandes PME (dans le contexte de cette étude, celles qui comptent entre 500 et 999 collaborateurs) étaient supposées être un peu moins bien armées pour faire face aux incidents que leurs homologues de plus grande taille (1 000 collaborateurs ou plus). Toutefois, d'après l'*Enquête sur l'efficacité des mesures de sécurité de Cisco*, les grandes PME ne se contentent pas seulement de copier le niveau de préparation des grandes entreprises en termes de sécurité dans bien des domaines. En effet, elles obtiennent souvent de meilleurs résultats, certainement grâce à leur flexibilité et à leur agilité accrues.

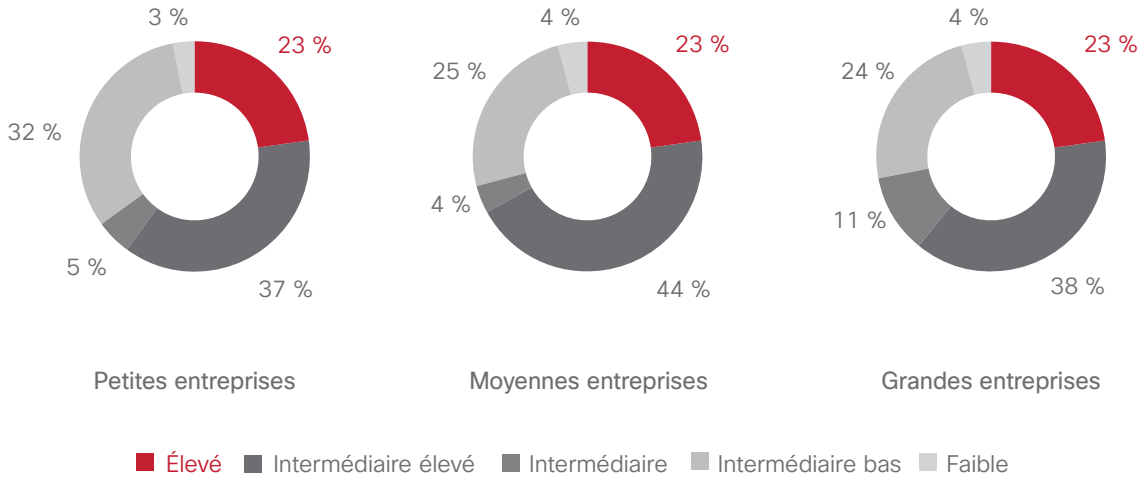
En fait, l'enquête révèle que les grandes PME sont plus susceptibles de développer des politiques de sécurité extrêmement sophistiquées. Comme l'illustre la Figure 36, un nombre considérablement plus important de grandes PME se hissent en haut du tableau et présentent un niveau de sophistication plus poussé que les petites PME (250 à 499 collaborateurs) et que les grandes entreprises (1 000 collaborateurs ou plus).

Cette tendance est prometteuse, car les PME sont le moteur de l'économie dans un contexte de reprise.

Les principales conclusions de l'enquête sur l'efficacité des PME et sur leur niveau de préparation en matière de sécurité :

- 92 % des PME disposent d'équipes internes chargées de faire face aux incidents. Dans la catégorie des grandes entreprises, ce chiffre s'élève à 93 %.
- 94 % des PME emploient un dirigeant directement responsable de la sécurité. Dans la catégorie des grandes entreprises, ce chiffre s'élève à 92 %.

Figure 36. Niveau de sophistication des politiques de sécurité des grandes PME



Les segments reflètent la hausse des niveaux de sophistication concernant la priorité de la sécurité dans l'entreprise et les conséquences pour les processus et les procédures.

Beaucoup plus de PME que de petites et grandes entreprises se trouvent dans les niveaux Élevé et Intermédiaire élevé.

Au moins 60 % possèdent des profils de sécurité plus sophistiqués.

Source : *Enquête sur l'efficacité des mesures de sécurité de Cisco*

3. Les tendances géopolitiques et du secteur

Nos experts en sécurité, géopolitique et politiques de protection identifient les tendances géopolitiques, actuelles et nouvelles, que les entreprises, et plus particulièrement les multinationales, devraient surveiller. Ils examinent également les derniers faits marquants concernant la souveraineté, la localisation, le cryptage et la compatibilité des données.

Pourquoi la cybercriminalité se développe dans les zones de faible gouvernance

Les RSSI et autres responsables de la sécurité ne se soucient guère de la dynamique géopolitique. Pourtant, ils devraient y prêter une attention toute particulière, surtout s'ils travaillent dans une multinationale. Ce qu'il se passe sur le plan géopolitique peut avoir une incidence directe sur les chaînes d'approvisionnement internationales et sur la gestion des données des clients et des collaborateurs dans différents pays. Par ailleurs, les coûts juridiques et réglementaires peuvent augmenter, des secrets commerciaux peuvent être volés, et enfin les risques physiques et les atteintes à la réputation peuvent se multiplier.

La cybercriminalité se développe dans le monde entier, et plus particulièrement dans les zones de faible gouvernance. L'Europe de l'Est, qui a longtemps été le berceau du crime organisé, est un exemple parmi d'autres. Dans les zones de faible gouvernance, il n'est pas rare de prouver l'existence de relations étroites entre les services publics de renseignement et des groupes organisés impliqués dans la cybercriminalité.

Selon les autorités américaines, certaines attaques récentes de grande envergure ayant ciblé des ressources aux États-Unis émanaient fort probablement de telles zones. Certaines attaques n'étaient pas menées dans l'optique de faire des profits. Il s'agissait plutôt de campagnes d'ordre politique ou visant à collecter des renseignements ou à infiltrer une infrastructure.[7] Cela laisse à penser que ces actions étaient sponsorisées par un état et/ou perpétrées par des organisations cybercriminelles sophistiquées.

De plus en plus d'administrations s'efforcent de renforcer la cybergouvernance par le biais de lois et de réglementations. La Chine, par exemple, a fait de l'« État de droit » le thème majeur de la 4e session plénière du XVIIIe congrès du parti communiste chinois (PCC).[8] Pékin s'est engagé à éradiquer la corruption et à appliquer les lois dans les entreprises et le gouvernement. Ces actions visent à une application plus rigoureuse de la loi et viennent soutenir les efforts internationaux déployés pour traquer et débusquer les cybercriminels.

L'Internet au service de groupes terroristes internationaux

L'émergence de groupes terroristes internationaux, comme l'État islamique (EI), constitue une autre tendance à surveiller. De tels groupes ne semblent pas être impliqués dans des activités cybercriminelles graves, mais ils font bon usage d'Internet, et surtout des médias sociaux, pour recruter leurs membres. Les principaux groupes terroristes transnationaux engrangent désormais suffisamment d'argent grâce à des activités « traditionnelles » comme l'extorsion de fonds et le trafic d'êtres humains et de pétrole. Toutefois, à mesure que ces organisations prennent de l'ampleur, elles peuvent basculer dans la cybercriminalité pour financer leurs actions dans le monde entier. Les jeunes organisations terroristes qui n'ont pas accès aux mêmes ressources que les groupes bien établis risquent également de se lancer dans la cybercriminalité pour accélérer leur croissance.

Consultez le billet de blog Cisco « Cupcakes and Cyberespionage » pour découvrir une nouvelle approche de la protection contre le cyberespionnage.

Concilier souveraineté, localisation et cryptage des données : un problème épineux

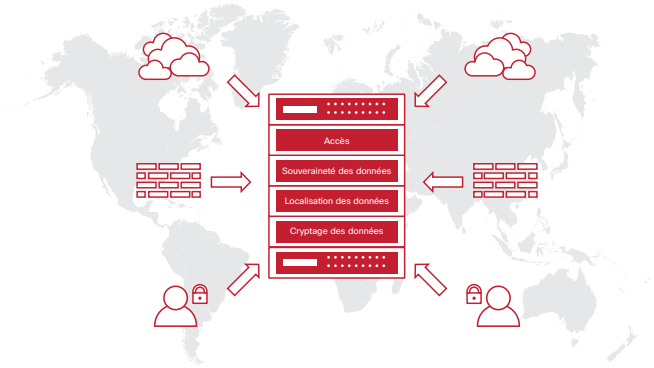
Les allégations d'Edward Snowden concernant la surveillance trop ambitieuse de l'administration américaine, la souveraineté des données (c'est-à-dire le fait que les données soient soumises à la juridiction du pays dans lequel elles sont stockées et pas à celle des gouvernements ou des tribunaux étrangers qui cherchent à y accéder unilatéralement) et la localisation des données (un gouvernement qui exige que les données soient stockées à un lieu précis) sont des sujets brûlants.

Certains pays veulent pouvoir localiser leurs données afin d'éviter que les administrations étrangères n'accèdent aux informations relatives à leurs citoyens. Ils élaborent des réglementations obligeant les données à rester à l'intérieur des frontières ou à être acheminées suivant des méthodes spécifiques. Les entreprises sont également contraintes d'utiliser du matériel fabriqué dans le pays.

À titre d'exemple, le Brésil a récemment promulgué une nouvelle loi qui « énonce des conditions de confidentialité qui interdisent largement aux entreprises [concernées] de partager les données personnelles des utilisateurs, leurs communications et certaines données de journalisation en ligne ».[9] Dans le même temps, la Russie a récemment amendé sa loi sur les informations et la protection des données qui impose à tous les opérateurs qui traitent les données personnelles des citoyens russes, y compris les données en ligne, de conserver des copies de ces données sur des serveurs et des bases de données en Russie. Cette loi doit entrer en vigueur en 2015.[10]

Face à ces lois nationales non interopérables régissant la localisation des données, les multinationales risquent d'être confrontées à des législations contradictoires. Respecter les exigences d'une nation en produisant, en conservant ou en supprimant des données peut constituer une infraction aux lois d'un autre pays.

Figure 37. Concilier souveraineté, localisation et cryptage des données : un problème épineux



Outre ces législations contradictoires, les exigences relatives à la localisation des données peuvent également restreindre la circulation des informations au-delà des frontières. Il en résulte une certaine confusion et d'énormes challenges en matière de gestion des réseaux. La chaîne d'approvisionnement entre également en ligne de compte : de plus en plus d'opérateurs de chaîne d'approvisionnement d'envergure internationale se dotent de technologies cloud pour connecter l'ensemble de leurs partenaires dans le monde entier. La localisation des données peut entraver, voire empêcher les échanges de données sur ces réseaux professionnels. Elle peut même gêner les activités transnationales de lutte contre la cybercriminalité.

De plus, certains pays choisissent d'utiliser uniquement des technologies développées localement ou limitent considérablement le nombre de personnes habilitées à traiter les données de leurs habitants. Cette situation risque de les couper du vivier de talents international, voire de limiter les innovations qui peuvent naître de l'échange de nouvelles idées.

Certains grands acteurs technologiques américains espèrent que le cryptage total apportera satisfaction à leurs clients, à savoir protéger leurs données pendant qu'elles transitent sur l'Internet sans frontières. Toutefois, le gouvernement américain a fait part de ses inquiétudes : un tel cryptage l'empêchera de protéger ses citoyens. Le nouveau directeur du GCHQ, le service de renseignements électronique du gouvernement britannique, qui s'apparente à la NSA (National Security Agency) aux États-Unis, a même suggéré que les géants américains des médias sociaux apportent leur aide dans la lutte contre le terrorisme en les autorisant à envoyer des communications cryptées dans le monde entier.[11]

Malgré ces critiques, les entreprises technologiques continuent de développer et d'adopter des mesures visant à regagner la confiance des clients. Elles agiront de la sorte jusqu'à ce que les pouvoirs publics aient mis en œuvre des politiques qui concilient la liberté d'expression et la protection des transactions, et la protection avancée contre les atteintes à la sécurité publique et nationale.

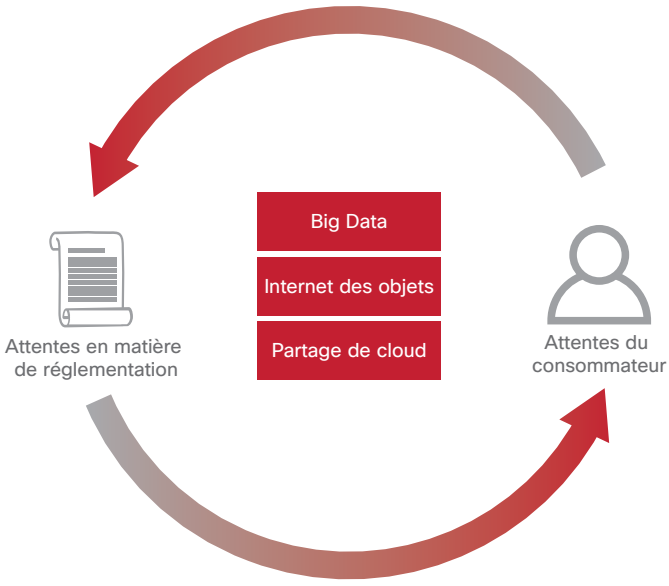
Il faut amener les pays, leurs gouvernements et leurs habitants à faire confiance aux produits technologiques et aux entreprises qui les développent pour leur prouver qu'ils sont protégés en toutes circonstances. Récemment, Mark Chandler, vice-président senior, directeur juridique et secrétaire Cisco, a écrit dans un billet de blog : « Il faut regagner la confiance en s'attaquant sérieusement à ces problèmes. Plus important encore, nous pourrons ainsi concrétiser les promesses de l'Internet de nouvelle génération, à savoir créer un monde dans lequel les relations entre les personnes et les appareils favorisent la liberté, la prospérité et les opportunités pour le monde entier. »[12]

L'harmonisation de la notion de confidentialité des données

L'attitude d'une personne ou d'une entreprise face à la confidentialité des données dépend en grande partie de sa localisation. Ces points de vue différents influencent la manière dont les pouvoirs publics réglementent la confidentialité des données et dont les entreprises mènent leurs activités lorsque ces réglementations sont en contradiction les unes avec les autres. Le ***rapport d'enquête sur l'indice de protection des données***, sponsorisé par Cisco et préparé par la Cloud Security Alliance, présente certains challenges auxquels sont confrontées les entreprises qui traitent des données stockées en ehors de leur propre pays ou des données qui appartiennent à des individus situés à l'étranger.

La question de l'harmonisation de la notion de confidentialité des données, c'est-à-dire la création d'approches cohérentes en matière de confidentialité au niveau international, doit être traitée de toute urgence en raison de la généralisation des services cloud. Admettons qu'une entreprise basée aux États-Unis achète un système de stockage cloud à une entreprise indienne. Si elle utilise ce cloud pour stocker les données de ses clients résidant en Allemagne, quelles lois s'appliquent ?

Figure 38. Respecter les diverses réglementations et les attentes du consommateur



L'Internet des objets et le Big Data sont d'autres facteurs qui poussent à trouver un terrain d'entente. Les entreprises cherchent de nouveaux moyens de connecter les appareils les uns aux autres et utilisent des jeux de données massifs pour prendre leurs décisions. Elles ont donc besoin de structures et de règles pour savoir comment gérer ces données à l'international.

D'importants efforts sont déployés pour harmoniser les règles régissant la confidentialité des données au sein d'une zone géographique ou d'un groupe de pays spécifique. Par exemple, l'Union Européenne met actuellement à jour son *règlement général sur la protection des données* pour harmoniser les diverses léglisations nationales en la matière. Tous les acteurs redoublent d'efforts pour parvenir à un consensus sur les lois concernant la souveraineté et la confidentialité des données. Une meilleure harmonisation serait la bienvenue, mais le texte final doit également être concret, en accord avec la réglementation d'autres régions et adapté aux nouvelles réalités technologiques. La Coopération économique pour l'Asie-Pacifique (APEC) a ratifié un accord visant à encadrer les flux transfrontaliers de données pour faciliter la coopération économique entre les pays de cette zone. Les états doivent s'atteler à atteindre un objectif plus général : créer des cadres régissant la confidentialité et la sécurité des données reposant sur des standards reconnus internationalement qui favorisent l'ouverture d'Internet et la libre circulation des données au-delà des frontières.

Si les états clarifient leur approche dans ces domaines, les entreprises pourront mieux appliquer des politiques de confidentialité des données à l'échelle internationale. Elles pourront également mettre en œuvre des stratégies plus efficaces d'intégration de la « protection de la vie privée dès la conception » (Privacy by Design) dans les produits et les services. Avec des législations claires et cohérentes, les entreprises pourront respecter les exigences en matière de confidentialité, voire aller au-delà, quel que soit le lieu de déploiement de leurs produits et de leurs services, favorisant ainsi le développement de produits innovants et l'utilisation des données.

La confidentialité des données : une compréhension partagée

Une enquête sur la protection des données a été menée auprès de spécialistes internationaux pour ces questions de confidentialité en Amérique du Nord, dans l'Union européenne et dans la zone Asie-Pacifique. Ils ont été interrogés sur la réglementation en vigueur sur leur territoire, sur les pratiques des pouvoirs publics, sur le contenu des utilisateurs et sur les standards de sécurité. Ils ont fait preuve de cohérence dans leurs réponses à la question visant à savoir s'ils comprenaient la signification de la confidentialité des données et la valeur des standards internationaux en la matière.

- **La localisation et la souveraineté des données :** pour les experts, les données personnelles et les informations nominatives ne doivent pas quitter le pays.
- **L'interception légale :** les experts sont tous d'accord sur les situations justifiant l'interception de données (par exemple, dans le cadre d'une enquête criminelle).
- **Le consentement des utilisateurs :** 73 % des personnes interrogées sont d'accord avec l'instauration d'une charte des droits de confidentialité des consommateurs, à l'échelle internationale et pas uniquement locale. 65 % d'entre elles déclarent que les Nations-Unies doivent s'engager activement dans la création d'une telle charte.
- **Les principes de confidentialité :** la question suivante a été posée aux experts : les principes de confidentialité de l'OCDE (Organisation de coopération et de développement économiques) faciliteraient-ils l'harmonisation des données ou, au contraire, renforceraient-ils les tensions ? Ils ont largement répondu en faveur de l'adoption de ces principes.

En résumé, l'enquête semble montrer que de nombreux experts approuvent les principes de base en matière de confidentialité, qui, s'ils étaient adoptés et standardisés à l'échelle internationale, pourraient favoriser l'activité, et non pas l'entraver. Les résultats indiquent également que les experts partagent tous l'idée de concevoir des principes de confidentialité pour les nouvelles solutions technologiques. Pour eux, il ne faut pas essayer d'adapter ces solutions aux exigences de confidentialité. Cependant, les cadres réglementaires actuels n'en sont qu'à leurs débuts et évoluent rapidement.

Si l'harmonisation devait s'améliorer, les entreprises et les individus en bénéficieraient. Toutefois, dans la mesure où ce secteur continue d'être le témoin de règles internationales discordantes, les entreprises devront se pencher plus attentivement sur les questions de protection et de confidentialité des données. Elles devront également adapter leurs offres et leurs processus de manière proactive pour répondre aux diverses réglementations et aux attentes du consommateur.

Pour en savoir plus sur la protection des données, lisez l'article « Data Protection in the Balance—EU Citizen Protection and Innovation » publié sur le blog Cisco Security.

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

Selon les experts en sécurité Cisco, il est temps pour les entreprises d'adopter une approche différente de la cybersécurité afin de renforcer leur niveau de protection. Elles doivent notamment envisager de nouvelles méthodes pour aligner le personnel, les processus et la technologie. La sécurité doit donc s'inviter dans les conseils d'administration pour conduire à l'adoption de contrôles de sécurité plus sophistiqués qui réduisent la surface d'attaque des terminaux et renforcent le réseau après une attaque.

Sécurité : savoir qui accède à votre réseau, quand et comment

Les RSSI et autres professionnels de la sécurité sont confrontés à des challenges complexes quant à l'accès aux informations et aux services du réseau. Avec la généralisation de la mobilité et du BYOD, ils doivent s'assurer que les collaborateurs peuvent accéder aux ressources de l'entreprise, où qu'ils se trouvent et quel que soit le mode de connexion au réseau.

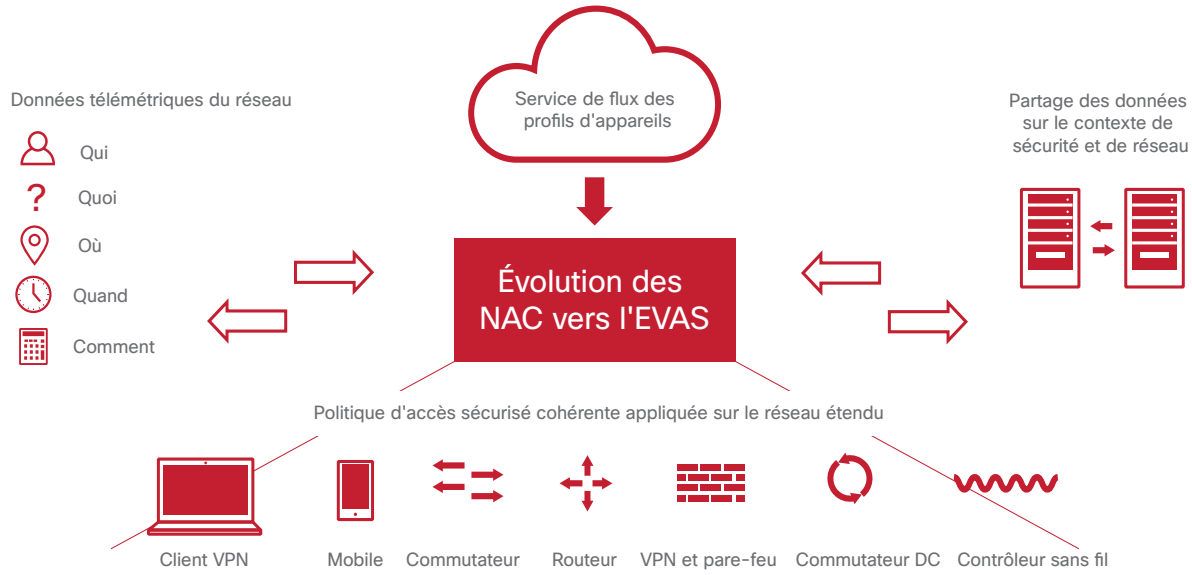
Les professionnels de la sécurité doivent aussi protéger le réseau contre les accès non autorisés et les cyberattaques, mais sans bloquer l'accès des utilisateurs légitimes. Par exemple, les réseaux VPN étaient utilisés d'office pour contrôler l'accès réseau. Cependant, certains d'entre eux impliquent des procédures complexes de connexion et l'achat de logiciels spéciaux, ce qui limite l'accès. De plus, de nombreux VPN ne permettent pas au département IT d'identifier la personne qui a eu accès au réseau, d'où elle s'est connectée et quel appareil elle a utilisé. Les VPN sont en pleine évolution : ils améliorent la visibilité, tout en assurant une expérience plus transparente pour l'utilisateur afin de renforcer la sécurité des terminaux.

Les contrôles d'accès réseau (NAC) qui assuraient une protection de base évoluent vers un rôle plus sophistiqué en matière de sécurité, d'accès et de visibilité sur les terminaux (EVAS). Contrairement aux technologies NAC plus anciennes, les contrôles EVAS utilisent des informations plus granulaires pour appliquer les politiques d'accès, comme des données sur le rôle de l'utilisateur, l'emplacement, les processus et la gestion des risques. Les contrôles EVAS permettent également aux administrateurs du réseau d'accorder un accès à des ordinateurs, mais également à des terminaux mobiles et à d'autres objets (IoT).

Ces contrôles sont à l'origine d'une approche de sécurité dans laquelle le réseau joue le rôle de capteur. Ils accordent ou interdisent l'accès à un réseau étendu, depuis un appareil distant (VPN) avant la connexion aux services réseau ou même depuis le réseau lui-même via des pools de ressources sensibles. Ils aident ainsi les entreprises à réduire la surface d'exposition du réseau et des terminaux, à limiter l'évolutivité et l'étendue d'une attaque, à corriger les problèmes et même à renforcer le réseau après une attaque.

Pour en savoir plus sur les solutions EVAS et découvrir comment elles permettent aux entreprises de mieux se protéger, lisez l'article « New White Paper from Enterprise Strategy Group on the Evolution of and Need for Secure Network Access » publié sur le blog Cisco Security.

Figure 39. L'évolution des contrôles d'accès au réseau (NAC) vers la visibilité, l'accès et la sécurité des terminaux (EVAS)



Avant une attaque, les contrôles EVAS peuvent :

- **Identifier les ressources à risques.** Surveiller toutes les ressources connectées au réseau à tout moment, identifier les utilisateurs, les appareils et les applications non conformes, et mettre ces informations en corrélation avec des outils tiers d'évaluation des vulnérabilités.
- **Réduire les risques.** Collecter toutes les informations exploitables à partager avec d'autres applications de réseau et de sécurité afin d'améliorer les workflows, de rationaliser les opérations et de hiérarchiser les activités correctives
- **Appliquer des politiques granulaires d'accès réseau.** Donner des informations sur le contexte qui permettent d'appliquer des politiques granulaires et de limiter l'accès au contenu, aux ressources ou aux segments de réseau sensibles.

Pendant une attaque, les contrôles EVAS peuvent :

- **S'intégrer dans des systèmes avancés de protection hébergés sur le réseau.** Partager des connaissances lorsque des activités malveillantes sont détectées afin de mettre en corrélation les données d'une attaque et les connexions, les configurations et les comportements des terminaux sur le long cours.
- **Bloquer la « chaîne de frappe » des systèmes compromis.** Limiter les attaques latérales en empêchant les systèmes compromis d'atteindre des ressources réseau non autorisées soumises à une politique dans le but de voler des identifiants, de remonter des privilèges et d'exfiltrer des données importantes.
- **Contenir une attaque.** Restreindre et mettre en quarantaine les systèmes ayant un comportement suspect.

Après une attaque, les contrôles EVAS peuvent :

- **Analyser les profils des terminaux pour rechercher des vulnérabilités.** Partager des informations de la base de données des contrôles EVAS avec des outils d'analyse des vulnérabilités pour aider les services IT à hiérarchiser l'application de correctifs.
- **Restaurer les systèmes compromis.** Lorsqu'ils sont intégrés dans des systèmes de gestion des informations des événements de sécurité (SIEM) et dans des systèmes de protection des terminaux, les contrôles EVAS peuvent automatiser l'application de correctifs et surveiller la progression.
- **Affiner les politiques d'accès et les contrôles de sécurité.** Exploiter des équipements de sécurité et de réseau pour segmenter le trafic des applications ou ajouter de nouvelles règles de pare-feu ou signatures IPS.

Contrairement aux anciens contrôles d'accès réseau extrêmement complexes, les solutions EVAS sont de véritables accélérateurs d'activité. Avec l'essor du BYOD, du cloud computing et de la mobilité, il est indispensable pour les entreprises d'améliorer la visibilité, d'en savoir plus sur les utilisateurs et les terminaux connectés, et d'appliquer plus efficacement les politiques de sécurité. Les experts en sécurité Cisco estiment que les RSSI privilégieront les solutions EVAS pour gérer les connexions complexes entre les utilisateurs, les appareils, les réseaux et les services cloud.

Le futur de la cybersécurité dépend de l'engagement des conseils d'administration aujourd'hui

D'après l'*Enquête sur l'efficacité des mesures de sécurité de Cisco*, 91 % des entreprises ont confié les rênes de la sécurité à un dirigeant. Toutefois, la sécurité doit continuer à gravir les échelons et à s'inviter dans les plus hautes sphères de l'entreprise : le conseil d'administration.

La cybersécurité a été récemment ajoutée à l'ordre du jour des conseils d'administration pour différentes raisons : des attaques massives touchant des entreprises bien connues, la multiplication des lois et des réglementations relatives à la sécurité des données, les tendances géopolitiques et les attentes des actionnaires. Un rapport rédigé par l'ISACA (Information Systems Audit and Control Association) a révélé que 55 % des directeurs doivent désormais considérer et gérer la cybersécurité comme une problématique à risque.[13]

Les responsables de la sécurité Cisco se félicitent de ce choix, mais regrettent le retard pris. Dans l'économie moderne, toutes les entreprises sont équipées de solutions IT. Par conséquent, les questions de sécurité ne sont pas uniquement du ressort du personnel dont la fonction intègre le terme « sécurité », mais bien de la responsabilité de tout le monde, du PDG au collaborateur fraîchement embauché. Chaque collaborateur doit se sentir concerné et savoir comment ne pas être victime d'attaque.

Les responsables de la sécurité Cisco affirment que le futur de la cybersécurité repose essentiellement sur un engagement plus fort du conseil d'administration. En effet, les directeurs, tous secteurs confondus, doivent connaître les risques en matière de cybersécurité et l'impact qu'ils peuvent avoir sur l'activité. Pour bien cerner l'ensemble des questions liées à la sécurité, certains conseils d'administration devront sans doute intégrer des spécialistes des technologies et de la cybersécurité.

Ils doivent également commencer à réfléchir aux contrôles de sécurité : *quels contrôles avons-nous mis en place ? Comment ont-ils été testés ? Avons-nous un processus de reporting en place ? Pouvons-nous détecter et corriger rapidement des compromissions inévitables ?* Et sans doute la question la plus importante : *que devons-nous encore savoir ?* Les DSI doivent se préparer à répondre à ces questions du conseil d'administration dans des termes auxquels tous les membres seront sensibles, tout en mettant en avant les implications pour l'entreprise.

Dans une récente interview réalisée par le magazine FORTUNE,[14] le responsable de la sécurité Cisco, John Stewart, a déclaré que ce type de questions posées par le conseil d'administration s'accompagne d'« un ensemble intéressant d'effets corollaires » qui permettent au secteur de gagner en maturité. Selon lui, la prochaine étape vitale, son espoir, sera d'amener les fabricants à intégrer la sécurité dans leurs produits.

John Stewart anticipe qu'avec le développement de l'Internet des objets, il y aura plus d'« appareils autonomes sur Internet que d'appareils commandés par des hommes », ce qui conduira forcément à des « accidents » potentiellement de forte magnitude. Intégrer la sécurité dans les produits permettra d'éviter nombre de ces problèmes, ou au moins d'en atténuer l'impact.

Les dirigeants d'entreprises technologiques doivent donc poser les questions suivantes à leurs responsables de la sécurité : *intégrons-nous la sécurité dans nos produits ? Si tel n'est pas le cas, quand pouvons-nous commencer ?*

Regardez le blog vidéo de John Stewart, le responsable de la sécurité chez Cisco, sur l'importance de la transparence des initiatives de cybersécurité et de la responsabilisation de tous les collaborateurs, jusqu'au conseil d'administration : http://blogs.cisco.com/security/ensuring-security-and-trust-stewardship-and-accountability.

Manifeste sur la sécurité Cisco : principes fondamentaux de protection contre les attaques du monde réel

Aujourd'hui, les RSSI doivent répondre à des questions délicates : *comment mon équipe peut-elle devenir le premier interlocuteur dans mon entreprise en cas d'incident ? Comment puis-je m'assurer que mon équipe dispose des outils et de la visibilité nécessaires pour hiérarchiser les problèmes et identifier les mesures à prendre ? Et comment protéger les utilisateurs (la clé de la réussite de mon entreprise) dans toutes les situations, même lorsqu'ils ne se trouvent pas sur site ?*

Les experts en sécurité Cisco recommandent aux RSSI de répondre à ces questions en mettant en œuvre et en respectant un ensemble de principes de sécurité, regroupés dans ce qu'ils appellent le Manifeste sur la sécurité.

Ces principes visent à aider les équipes chargées de la sécurité et les utilisateurs de leur entreprise à mieux cerner et à relever les challenges liés à la cybersécurité. Ils peuvent servir de point de départ aux entreprises qui cherchent à développer des approches plus dynamiques de la sécurité et à faire preuve d'une capacité d'adaptation et d'innovation plus poussée que leurs concurrents :

1. **La sécurité doit être considérée comme un levier de croissance pour l'entreprise.** La sécurité ne doit jamais constituer un obstacle ni être source de complexité, ce qui pourrait nuire à la productivité et à l'innovation. Pourtant, ce n'est pas le cas des solutions technologiques imposées par les équipes chargées de la sécurité. Première cause : les équipes ne sont invitées que tardivement, voire pas du tout, aux discussions portant sur le déploiement d'une nouvelle technologie. Toutefois, les professionnels de la sécurité sont également fautifs parce qu'ils attendent une invitation qu'ils ne recevront certainement jamais. Ils devraient plutôt anticiper et s'impliquer dans les débats. Ils pourraient ainsi démontrer que les processus de sécurité contribuent à l'agilité et à la réussite de l'entreprise en plus de protéger ses données, ses ressources et son image.
2. **La solution de sécurité doit fonctionner avec l'architecture en place et être exploitable.** Les équipes chargées de la sécurité ne devraient pas avoir à concevoir une architecture adaptée aux nouvelles solutions technologiques supposées renforcer la protection. Les architectures impliquent inévitablement des contraintes. Les entreprises ne devraient pas avoir à modifier leur mode de fonctionnement pour s'adapter aux nouvelles technologies de sécurité, ni à se voir interdire de travailler autrement en raison des technologies déjà en place. Cette « surcharge d'architecture » pousserait les utilisateurs à contourner les systèmes de sécurité, ce qui exposerait davantage l'entreprise. De plus, si une technologie de sécurité est trop difficile à comprendre pour les utilisateurs et doit être gérée par de rares collaborateurs spécialisés et compétents, l'entreprise n'en tirera aucun bénéfice.
3. **La sécurité doit être transparente et instructive.** Les utilisateurs doivent pouvoir avoir des informations sur les raisons qui les empêchent d'effectuer une tâche particulière. Ils doivent aussi comprendre comment agir en toute sécurité au lieu de contourner la protection en place sous prétexte qu'ils doivent faire leur travail. Par exemple, si un utilisateur essaie d'accéder à une page web et voit le message suivant s'afficher, « L'accès à ce site a été interdit par l'administrateur », il ne sait pas pourquoi l'accès lui est refusé. En revanche, si le message déclare, « L'accès à ce site a été interdit parce qu'il a servi à diffuser des programmes malveillants au cours des 48 dernières heures », l'utilisateur sera mieux informé des risques pour son entreprise, mais aussi pour lui personnellement. Les technologies de sécurité doivent aider les utilisateurs à atteindre leurs objectifs en toute sécurité par le biais de recommandations claires ou en les dirigeant vers les interlocuteurs appropriés qui les aideront en temps opportun.
4. **L'architecture doit fournir une visibilité et des mesures appropriées.** Grâce à une architecture ouverte, les équipes chargées de la sécurité peuvent déterminer l'efficacité des solutions. Les professionnels de la sécurité ont aussi besoin d'outils pour automatiser la visibilité sur le réseau. Ils peuvent ainsi tracer le trafic et les ressources du réseau. Par une meilleure compréhension du fonctionnement des technologies de sécurité et par l'identification des comportements normaux (et anormaux) de l'environnement IT, les équipes peuvent réduire les tâches d'administration. Elles peuvent par ailleurs identifier les attaques, réagir et adapter leurs mécanismes de défense de façon plus dynamique et plus précise. Grâce à cette approche, les équipes chargées de la sécurité peuvent pleinement tirer parti de contrôles plus pertinents et plus ciblés qui contribuent à résoudre les problèmes.
5. **La sécurité doit être considérée comme un « problème humain ».** Une approche de sécurité axée sur la technologie n'améliore pas le niveau de protection. Au contraire, elle ne fait qu'empirer les choses. Les technologies sont simplement des outils qui aident les utilisateurs à mieux protéger leur environnement. Les équipes chargées de la sécurité doivent former les utilisateurs aux réflexes à adopter où qu'ils se trouvent (au bureau, à domicile, en déplacement). Ils pourront ainsi prendre les bonnes décisions et demander de l'aide en temps opportun lorsqu'ils détectent un comportement anormal. L'instauration d'un dialogue plus ouvert entre les professionnels de la sécurité et les utilisateurs permet également à ces derniers de comprendre que la technologie ne peut pas garantir la sécurité à elle seule. Les personnes, les processus et les technologies doivent assurer ensemble la protection. Tous les utilisateurs de l'entreprise doivent s'engager et rester vigilants, quelle que soit leur position hiérarchique : la sécurité est l'affaire de tous.

Le manifeste sur la sécurité Cisco est un appel au changement. Dans le monde réel, la technologie, les politiques et les bonnes pratiques doivent renforcer la protection dans l'ensemble de l'entreprise et favoriser des décisions plus éclairées concernant les risques. Grâce à des principes directeurs forts, les utilisateurs comprennent bien pourquoi ils n'ont pas le droit de faire certaines choses et quelles seraient les conséquences pour l'entreprise s'ils contournaient les mesures de sécurité.

Le manifeste sur la sécurité Cisco ou tout document qui reprend ses principes fondamentaux permet aux utilisateurs et aux spécialistes de la sécurité de connaître les tenants et les aboutissants : même si de nombreuses attaques peuvent être évitées, certaines compromissions sont inéluctables, mais vous pouvez y remédier très rapidement. L'objectif consiste à réduire le délai de résolution d'un incident et pas uniquement à chercher à les empêcher de se produire.

À propos de Cisco

Cisco crée des solutions de cybersécurité intelligentes et concrètes. Nous proposons désormais l'une des gammes de solutions de protection avancée les plus complètes du marché couvrant un vaste éventail de vecteurs d'attaque. Notre approche axée sur les menaces et les aspects opérationnels réduit la complexité et la fragmentation, tout en vous apportant une visibilité avancée, un contrôle systématique et une protection renforcée avant, pendant et après l'attaque.

Les chercheurs spécialisés de notre écosystème de sécurité adaptative et collective regroupent l'ensemble des informations sur les risques identifiés en étudiant les données télémétriques émanant des nombreux appareils et capteurs, des flux publics et privés, et de la communauté open source Cisco. Tous les jours, des milliards de requêtes web et des millions d'e-mails, d'échantillons de programmes malveillants et d'intrusions réseau sont collectés.

Notre infrastructure et nos systèmes sophistiqués analysent ces données télémétriques pour permettre aux chercheurs et aux systèmes automatisés de détecter les attaques et d'en identifier les causes et l'envergure où qu'elles se produisent : réseaux, Internet, data centers, terminaux, terminaux mobiles, systèmes virtuels, e-mails et cloud. L'analyse de ces données nous permet de renforcer en temps réel la sécurité des produits et des services que nos clients utilisent dans le monde entier.

Notre système de sécurité adaptative et collective est alimenté par plusieurs groupes aux statuts différents : Talos, Security & Trust Organization, Managed Threat Defense (MTD) et Security Research and Operations (SR&O).

Pour en savoir plus sur notre approche axée sur les menaces, rendez-vous sur **www.cisco.com/go/security**.

Annexe

Autres conclusions de l'enquête sur l'efficacité des mesures de sécurité

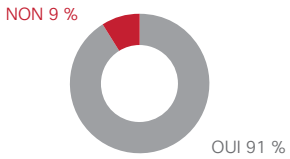
Ressources

Le budget dédié à la sécurité fait-il partie du budget IT ? Membres de départements IT n=1 720

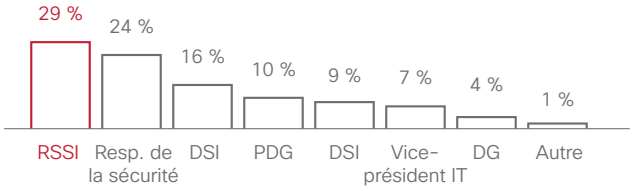
Politiques, procédures et opérations de sécurité

Le dirigeant le plus haut placé chargé de la sécurité est le plus souvent un RSSI ou un responsable de la sécurité.

Un dirigeant de votre entreprise est-il directement responsable de la sécurité ?
Personnes interrogées déclarant que les responsabilités et les rôles sont clairs ; n=1 603



Appellation de poste
Personnes interrogées déclarant qu'un dirigeant est responsable de la sécurité ; n=1 465



Dans les entreprises du secteur de la santé, on est moins susceptible de savoir quel responsable est chargé de la sécurité.

Partager le rapport

Pour près des deux tiers des personnes interrogées, la sécurité est une priorité pour les dirigeants d'entreprises.

Engagement des dirigeants n=1738	Équipes chargées de la sécurité n=797			RSSI n=941		
	Pas d'accord	D'accord	Tout à fait d'accord	Pas d'accord	D'accord	Tout à fait d'accord
Les dirigeants de mon entreprise considèrent la sécurité comme une haute priorité	8 %	34 %	58 %	3 %	30 %	67 %
Les rôles et responsabilités en matière de sécurité sont clairs dans l'équipe de direction de mon entreprise	9 %	39 %	52 %	2 %	32 %	64 %
L'équipe de direction de mon entreprise a établi des mesures claires pour l'évaluation de l'efficacité de notre stratégie de sécurité	11 %	44 %	45 %	4 %	37 %	59 %

Les personnes interrogées signalant n'ayant pas eu à faire face à la méfiance du public suite à la découverte d'une faille dans la sécurité de l'entreprise sont plus nombreuses à être tout à fait d'accord avec l'affirmation « Les dirigeants de mon entreprise considèrent la sécurité comme une haute priorité ».

Un pourcentage élevé considère que les processus de sécurité en place encouragent la participation des employés.

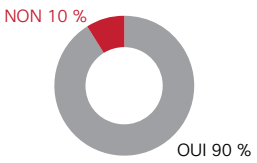
Processus de sécurité n=1738	Équipes chargées de la sécurité n=797			RSSI n=941		
	Pas d'accord	D'accord	Tout à fait d'accord	Pas d'accord	D'accord	Tout à fait d'accord
Les responsables des entités commerciales sont encouragés à contribuer à la mise en place des politiques et des procédures de sécurité	12 %	39 %	49 %	6 %	40 %	54 %
Mon entreprise est capable de détecter les vulnérabilités des dispositifs de sécurité avant un incident	13 %	43 %	44 %	4 %	39 %	57 %
Les employés de mon entreprise sont encouragés à signaler les pannes et les problèmes de sécurité	11 %	34 %	55 %	4 %	36 %	60 %
Les processus et les procédures de sécurité de mon entreprise sont clairs et bien compris	13 %	39 %	48 %	4 %	37 %	59 %
Les processus de sécurité de mon entreprise nous permettent d'anticiper et d'éliminer les problèmes avant qu'ils ne nous affectent	14 %	40 %	46 %	3 %	40 %	47 %
Les processus de sécurité de mon entreprise sont mesurés et contrôlés à partir de données quantitatives	13 %	40 %	47 %	4 %	35 %	61 %
Mon entreprise a optimisé ses processus de sécurité et se consacre désormais à leur amélioration	12 %	42 %	46 %	4 %	36 %	60 %

Les professionnels de la sécurité des PME ont tendance à être plus souvent tout à fait d'accord avec les affirmations sur les processus de sécurité que les professionnels des grandes entreprises.

9 personnes interrogées sur 10 indiquent que les équipes de sécurité suivent des formations régulières. Les formations sont généralement dispensées par des équipes internes.

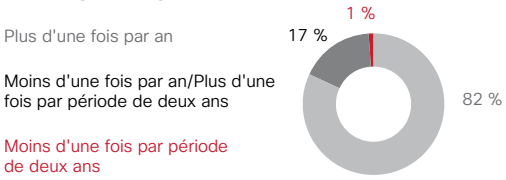
Le personnel chargé de la sécurité connaît-il le contexte et/ou suit-il des programmes de formation à la sécurité régulièrement ?

Personnes interrogées chargées de la sécurité ; n=1 726



À quelle fréquence une formation à la sécurité est-elle dispensée ?

Personnes interrogées chargées de la sécurité ; n=1556

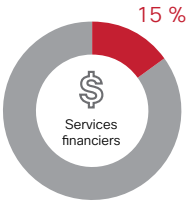


Qui dispense la formation à la sécurité ?

Personnes interrogées dont les équipes dédiées à la sécurité reçoivent une formation ; n=1 556

Équipe interne chargée de la sécurité 79 % | Sous-traitants 38 % | Ressources humaines 25 % | Autres employés 10 % | Autres 1 %

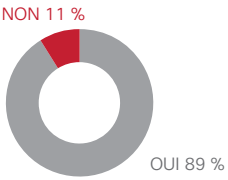
15 % des professionnels des services financiers déclarent ne pas recevoir de formation à la sécurité régulièrement.



Le personnel assiste régulièrement à des réunions ou à des formations. Près de deux tiers affirment faire partie d'associations du secteur de la sécurité.

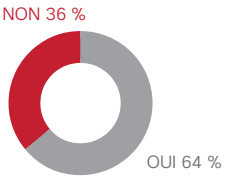
Le personnel dédié à la sécurité assiste-t-il à des conférences et/ou à des formations externes pour améliorer et entretenir ses compétences ?

Personnes interrogées chargées de la sécurité ; n=1715



Les employés participent-ils à des conseils ou comités sur la sécurité ?

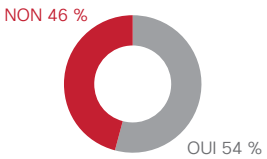
Personnes interrogées chargées de la sécurité ; n=1690



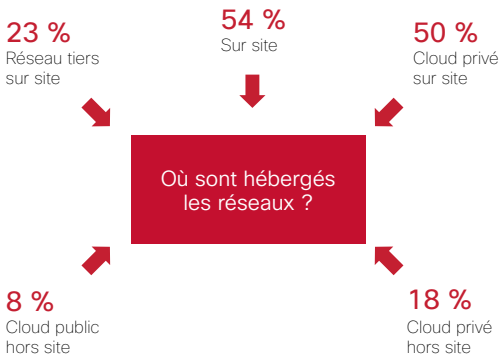
Plus de la moitié des personnes interrogées déclarent que leur entreprise a eu à faire face à la méfiance du public après la découverte d'une faille.

Votre entreprise a-t-elle déjà dû faire face à la méfiance du public après la découverte d'une faille ?

Personnes interrogées chargées de la sécurité ; n=1701



L'hébergement sur site des réseaux de l'entreprise est le plus fréquent. Moins d'une entreprise sur dix déclare héberger son réseau sur un cloud public.



Beaucoup plus de responsables des opérations de sécurité que de RSSI interrogés indiquent que leur entreprise a recours à un hébergement hors site (cloud privé et public).

Sophistication

Les résultats des segments varient de façon prévisible au niveau de nombreuses mesures du degré de sophistication de la sécurité…

	Faible	Intermédiaire bas	Intermé-diaire	Intermédiaire élevé	Élevé
Les dirigeants des entreprises considèrent la sécurité comme une priorité	22 %	38 %	45 %	71 %	81 %
… et utilisent des mesures claires pour l'évaluation de l'efficacité de leur stratégie de sécurité	17 %	19 %	32 %	52 %	79 %
L'entreprise suit des processus/procédures de sécurité clairs et bien compris	0 %	22 %	15 %	72 %	88 %
… mesurés et contrôlés à partir de données quantitatives	0 %	17 %	33 %	65 %	76 %
… et examine régulièrement ses pratiques et outils de sécurité pour s'assurer qu'ils sont à jour et efficaces	0 %	17 %	33 %	65 %	76 %
L'entreprise gère très bien la sécurité de la RH (nouveaux venus et bons processus pour les transferts et les départs)	16 %	27 %	36 %	52 %	76 %
Les informations sont répertoriées et classées clairement	17 %	26 %	40 %	58 %	73 %
Les installations IT de mon entreprise sont bien protégées	17 %	21 %	41 %	63 %	80 %
Les technologies de sécurité sont bien intégrées et fonctionnent efficacement	17 %	21 %	38 %	59 %	78 %
… l'entreprise est capable de détecter les vulnérabilités des dispositifs de sécurité avant un incident potentiel	0 %	23 %	25 %	63 %	70 %

Mais pas toujours…

	Faible	Intermédiaire bas	Intermé-diaire	Intermédiaire élevé	Élevé
Un dirigeant de votre entreprise est directement responsable de la sécurité	85 %	91 %	88 %	93 %	93 %
L'entreprise possède une stratégie de sécurité écrite et formelle, à l'échelle de l'entreprise qui est revue régulièrement	59 %	47 %	58 %	65 %	60 %
L'entreprise possède une stratégie de sécurité écrite et formelle, à l'échelle de l'entreprise qui est revue régulièrement	47 %	44 %	50 %	59 %	54 %

Notes

1. *Rapport Cisco sur la cybersécurité du premier semestre 2014 :* www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
2. Pour en savoir plus sur les vulnérabilités des systèmes de gestion de contenu, consultez « Wordpress Vulnerabilities : Who Is Minding the Store ? », *Rapport Cisco sur la cybersécurité du premier semestre 2014 :* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
3. « Goon/Infinity/RIG Exploit Kit Activity », Cisco IntelliShield : bulletin de sécurité, juillet 2014 : http://tools.cisco.com/security/center/mviewAlert.x?alertId=34999.
4. *Rapport Cisco sur la cybersécurité du premier semestre 2014 :* www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
5. « Cisco Event Response : POODLE Vulnerability », 15 octobre 2014 : http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Poodle_10152014.html.
6. « OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations » blog Cisco Security, 9 avril 2014 : http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations
7. « JP Morgan and Other Banks Struck by Hackers », par Nicole Perlroth, *The New York Times,* 27 août 2014 : www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html?_r=0 ; « 'Trojan Horse' Bug Lurking in Vital U.S. Computers Since 2011 », par Jack Cloherty et Pierre Thomas, ABC News, 6 novembre 2014 : http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476.
8. « 4 Things We Learned from China's 4th Plenum », par Shannon Tiezzi, *The Diplomat,* 23 octobre 2014 : http://thediplomat.com/2014/10/4-things-we-learned-from-chinas-4th-plenum/.
9. « Brazil's New Internet Law Could Broadly Impact Online Privacy and Data Handling Practices » *Chronicle of Data Protection,* 16 mai 2014 : www.hldataprotection.com/2014/05/articles/international-eu-privacy/marco-civil-da-internet-brazils-new-internet-law-could-broadly-impact-online-companies-privacy-and-data-handling-practices/.
10. « Russian data localization law may now come into force one year ahead of schedule, in September 2015 », par Hogan Lovells, Natalia Gulyaeva, Maria Sedykh et Bret S. Cohen, Lexology.com, 18 décembre 2014 : www.lexology.com/library/detail.aspx?g=849ca1a9-2aa2-42a7-902f-32e140af9d1e.
11. « GCHQ Chief Accuses U.S. Tech Giants of Becoming Terrorists' 'Networks of Choice' », par Ben Quinn, James Ball et Dominic Rushe, *The Guardian,* 3 novembre 2014 : www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan.
12. « Internet Security Necessary for Global Technology Economy », par Mark Chandler, blog Cisco, 13 mai 2014 : http://blogs.cisco.com/news/internet-security-necessary-for-global-technology-economy.
13. « Cybersecurity : What the Board of Directors Needs to Ask », ISACA et la fondation de recherche IIA, août 2014 : www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx.
14. « It's Time for Corporate Boards to Tackle Cybersecurity. Here's Why », par Andrew Nusca, Fortune Magazine, 25 avril 2014 : http://fortune.com/2014/04/25/its-time-for-corporate-boards-to-tackle-cybersecurity-heres-why/.

Siège social aux États-Unis
Cisco Systems
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.