www.steria.com

Communiqué de presse

Etude Steria : L'excès de confiance menace-t-il la sécurité des entreprises européennes ?

L'essentiel

L'enquête Steria réalisée auprès de 270 décideurs en sécurité révèle que 91 % des entreprises européennes s'estiment capables de faire face à une crise majeure de sécurité. Mais entre la confiance affichée et la réalité des pratiques, la cohérence n'est pas totale. En effet, les entreprises n'ont pas pris les mesures adhoc les plus élémentaires pour traiter les crises lorsqu'elles surviennent. Ainsi, seules 27 % d'entre elles opèrent leur sécurité en 24/7 dont moins d'un quart des répondants français.

Dans ce contexte, des points positifs émergent pour l'avenir : les arbitrages budgétaires se font en faveur de la sécurité et la sécurité est positionnée à haut niveau dans les entreprises, ce qui favorise la mise en œuvre de stratégies ambitieuses répondant aux enjeux business. Et même si la mesure de la performance reste fortement focalisée sur le contrôle des coûts, l'amélioration de la détection des attaques est la 2e motivation à l'externalisation parmi les entreprises de plus de 5000 collaborateurs.

Paris, France – 30 janvier 2014 – Avec la révolution digitale sont apparus de nouvelles technologies et de nouveaux usages : mobilité, Cloud, réseaux sociaux, Big Data… Cette ouverture expose les informations de l'entreprise, fait croître les convoitises et suscite l'intérêt des groupes malveillants. Plus importants que jamais, les cyber-risques se multiplient : en 2012, les attaques ciblées ont augmenté de 42 % dans le monde, portant désormais également atteinte à la compétitivité ou à la réputation des entreprises. On estime à 110 milliards de dollars les pertes financières dues à la cybercriminalité à l'échelle mondiale.

Dans ce contexte, l'étude Steria sur la cyber-sécurité en Europe, menée auprès de 270 décideurs en sécurité représentant petites, moyennes et grandes entreprises en France, au Royaume-Uni, en Allemagne et en Norvège, révèle où les entreprises européennes se situent aujourd'hui en matière de cyber sécurité et leurs anticipations à court et moyen termes. Ont-elles pris la mesure des attaques auxquelles elles seront de plus en plus confrontées ? Sont-elles préparées pour supporter des crises majeures ?

Même s'il est illusoire d'envisager une protection totale, ont-elles mis en place les moyens nécessaires et adaptés pour prévenir les risques, détecter les menaces et se protéger contre les attaques ? Ont-elles accès aux bonnes ressources et aux bonnes offres de la part des professionnels de la sécurité ?

Les entreprises européennes sont face à une réelle prise de conscience vis-à-vis des attaques auxquelles elles seront de plus en plus confrontées.

Alors même que les attaques externes se multiplient, les attaques internes restent encore les plus redoutées par les entreprises européennes, et plus fortement en France. Ainsi, encore plus de 50 % des entreprises considèrent que les attaques externes représentent moins de 20 % des menaces.

Pour près de la moitié des entreprises françaises, l'enjeu majeur est de protéger leurs avantages compétitifs, particulièrement contre le vol de données, au centre de toutes les préoccupations de 60 % des décideurs, aujourd'hui et pour les 3 ans à venir. L'effet Prism, Bullrun, Mandiant est bien présent. Parmi les attaques externes, l'espionnage IT est la menace plus redoutée pour 37 % des entreprises. Les « APT » (Advanced Persistent Threat), la menace en 3 lettres qui devrait faire trembler les responsables sécurité n'est en revanche pas encore identifiée parmi les risques majeurs.

Les entreprises françaises et européennes sont confiantes sur leur avenir en matière de sécurité tant sur le plan de la disponibilité des ressources que des budgets et sur leur capacité à supporter des risques majeurs

Les entreprises européennes affichent une sérénité élevée dans l'éventualité d'une crise majeure de sécurité, 91 % d'entre elles s'estiment prêtes à y faire face et quasiment tout autant dans l'Hexagone.

De plus, les budgets sécurité restent et devraient rester préservés : moins d'un tiers des entreprises interrogées anticipent une baisse. 85 % des répondants européens et 90 % des décideurs français, considèrent qu'ils auront le budget sécurité adéquat dans les 3 prochaines années.

Mais la confiance affichée n'est pas en totale adéquation avec la réalité des pratiques… Les entreprises n'ont pas encore pris toutes les mesures adhoc nécessaires pour traiter les crises lorsqu'elles surviennent.

La sécurité opérée en 24/7 n'est pas encore la référence, seul le quart des entreprises interrogées l'a mise en place, aussi bien en France qu'au niveau européen. Et même les plus grandes entreprises sont moins de la moitié à en bénéficier.

Seules **14 %** des entreprises de moins de 5000 personnes disposent d'un Centre Opérationnel de Sécurité (SOC) leur permettant de détecter les cyber-attaques et de réagir en cas de crise majeure de sécurité.

Cependant, le contexte légal favorable en France soutient le développement des SOC : 14 % des décideurs français déclarent avoir un tel projet dans les 3 ans à venir, loin devant l'Allemagne (5,6 %), le Royaume-Uni (4,1 %) et la Norvège (2,5 %).

Enfin, seuls **15 %** des sondés estiment avoir une assurance couvrant les cyber-risques, ce type d'assurance étant généralement jugée trop complexe.

Face aux risques, les entreprises comptent encore beaucoup sur elles-mêmes aujourd'hui, mais d'ici 5 ans la sécurité devrait être principalement traitée par des prestataires externes, avec une plus grande mutualisation des moyens.

Aujourd'hui les entreprises européennes identifient des freins structurels à l'externalisation et les offres des industriels semblent manquer de maturité: 20 % des entreprises ne trouvent pas encore d'offre d'externalisation adaptée à leurs besoins. Mais lorsqu'elles se projettent, les entreprises considèrent plus facilement l'externalisation, et plus de 2/3 d'entre elles déclarent qu'elles externaliseront une partie de leur activité de sécurité dans le futur et ¾ en France.

C'est d'abord la réduction des coûts qui parle pour l'externalisation. Mais l'amélioration de la détection des attaques est la 2e motivation à l'externalisation parmi les entreprises de plus de 5000 employés.

D'ici cinq ans, la sécurité devrait être principalement traitée par des prestataires externes pour plus d'une entreprise sur quatre. A même échéance, la mutualisation des capacités de sécurité entre entreprises de mêmes secteurs d'activité devrait commencer à devenir une réalité : 15 % des entreprises interrogées l'envisagent.

« *La mutualisation de la sécurité des entreprises, notamment à travers l'externalisation, devient aujourd'hui une nécessité pour accéder aux meilleures capacités et compétences face aux nouvelles cyber-menaces»,* ajoute **Florent Skrabacz**.

« Au-delà de la simple réduction des coûts, elle permettra aux entreprises de bénéficier des dernières innovations en matière de détection des attaques, ainsi que du savoir-faire des professionnels les plus expérimentés. Néanmoins, les prestataires de services externes devront rassurer les entreprises qui considèrent que la sécurité de leurs informations est trop critique pour être confiée à des tiers, et les convaincre que leurs politiques de sécurité doivent leur permettre d'être plus agile face aux cyber-risques ».

A propos de l'étude :
Steria, accompagné par Pierre Audoin Consultant (PAC), a publié un rapport indépendant sur la cyber sécurité mettant en perspective les stratégies et modèles de cyber sécurité à un horizon de trois ans. L'objectif est de montrer la réalité de la perception des menaces par les entreprises européennes et l'adéquation des moyens mis en œuvre pour y faire face. Ce rapport est basé sur une étude menée auprès de 270 décideurs en sécurité. Ils représentent des petites et moyennes entreprises ainsi que des Grands Comptes de tous secteurs d'activité situés en France, au Royaume-Uni, en Allemagne et en Norvège. L'étude se compose d'une phase quantitative et d'une phase qualitative. La phase quantitative repose sur 250 entretiens téléphoniques répartis de la manière suivante : 70 interviews en France, 70 au Royaume-Uni, 70 en Allemagne et 40 en Norvège. Par ailleurs, PAC a procédé à 20 entretiens approfondis en face-à-face. Basés sur le même questionnaire que les entretiens quantitatifs, ils ont pu permettre aux décideurs en sécurité de grandes entreprises et d'organisations gouvernementales spécialisées, de développer leur stratégie de cyber sécurité et les modalités de sa mise en œuvre.

Les conclusions de l'étude sont disponibles à l'adresse : http://www.steria.com/fr/rapportcybersecurite

###

A propos de Steria: www.steria.com
Steria délivre des services IT dédiés aux entreprises et se positionne comme le partenaire de confiance de la transformation d'un grand nombre d'organisations privées comme d'administrations à travers le monde. Steria délivre des services qui s'appuient sur les nouvelles technologies et qui permettent aux administrations et aux entreprises d'améliorer leur efficacité et leur rentabilité. Grâce à une excellente connaissance des activités de ses clients et son expertise des technologies de l'information et de l'externalisation des processus métiers de l'entreprise, Steria fait siens les défis de ses clients et les aide à développer des solutions innovantes pour y faire face. De par son approche collaborative du conseil, Steria travaille avec ses clients pour transformer leur organisation et leur permettre de se focaliser sur ce qu'ils font le mieux.

Les 20 000 collaborateurs de Steria, répartis dans 16 pays, prennent en charge les systèmes, les services et les processus qui facilitent la vie quotidienne de millions de personnes chaque jour. Créé en 1969, Steria est présent en Europe, en Inde, en Afrique du Nord et en Asie du Sud-Est. Le Groupe a réalisé un chiffre d'affaires de 1,83 milliard d'euros en 2012. Son capital est détenu à plus de 20 %(*) par ses collaborateurs. Steria, dont le siège social est basé à Paris, est coté sur Euronext Paris.
(*): Dont les « SET Trust » et « XEBT Trust » (4,15% du capital)

Contacts presse :
Burson-Marsteller i&e - Tél. : 01 56 03 12 44/ 13 38
Henry de Romans / Benjamin Puygrenier
henry.de-romans@bm.com / benjamin.puygrenier@bm.com

Steria – Tél. : 01 34 88 57 64
Amandine Mouillet / Coralie Bitan
Amandine.mouillet@steria.com / coralie.bitan@steria.com

Toutes les actualités de Steria sont également sur :