



*“opinionway*

Communiqué de Presse

AL'X COMMUNICATION - Véronique Loquet  
06 68 42 79 68 vloquet@alx-communication.com

## La nouvelle édition du baromètre annuel du CESIN révèle l'impact majeur de la transformation numérique sur la gestion des données sensibles des entreprises

Le Club des Experts de la Sécurité de l'Information et du Numérique dévoile les résultats de sa deuxième grande enquête OpinionWay pour le CESIN.

**Paris, le 24 janvier 2017** – Afin de mieux cerner la perception de la cyber-sécurité et de ses enjeux au sein des grandes entreprises françaises, le CESIN a mis en place un baromètre annuel. Le Club dévoile ainsi pour la deuxième année consécutive, les résultats d'une grande enquête indépendante, menée auprès de ses membres, Responsables Sécurité des Systèmes d'Information (RSSI) des grands groupes français.

Le sondage OpinionWay pour le CESIN a ciblé 280 membres de l'association, et les résultats de l'étude portent sur un échantillon de 141 répondants. Quatre grandes thématiques sont étudiées : l'évolution des cyber-attaques, l'efficacité des solutions techniques, les perspectives pour l'avenir avec les enjeux de la transformation numérique, et la gouvernance cyber dans les entreprises.

Le nombre de cyber-attaques constatées est en hausse pour 46% des entreprises. **Le Ransomware conserve sa position d'attaque la plus fréquente.** 80% des entreprises ont subi des demandes de rançon, dont la volumétrie croit à nouveau de +19 points par rapport à l'année passée, loin devant le déni de service qui a touché 40 % des entreprises et se trouve au deuxième rang du classement, suivi par les attaques virales générales. A contre-courant, on constate une baisse des attaques ciblées et du vol de données personnelles, soulignant un décalage entre la réalité du terrain et la prégnance de ce phénomène dans les médias liés à des attaques d'envergure subies plus particulièrement par les gros acteurs du web. Par ailleurs le social engineering et les vulnérabilités résiduelles permanentes touchent elles, une entreprise sur deux.

**Face aux menaces grandissantes, le marché de la cybersécurité doit persévérer dans son évolution.** 40% des entreprises jugent les solutions techniques insuffisamment adaptées aux types et à la fréquence actuelle des attaques. La détection reste un axe majeur de la cyber-sécurité avec la mise en place d'outils de log management et de supervision montrant une réelle avancée des entreprises pour anticiper les dangers, tandis que la gestion du risque cyber évolue, un quart des entreprises ayant souscrit une cyber-assurance, et 17% l'envisagent d'ici un an.

**Dans ce contexte, les dynamiques de transformation numérique impactent significativement la gestion des données sensibles pour 89 % des RSSI interrogés.**

Le Cloud adopté par un très grand nombre d'entreprises implique des risques et mesures spécifiques. Un sujet qui préoccupe vivement les RSSI, notamment pour le contrôle d'accès, la localisation du stockage en dehors des frontières de l'Union Européenne et de fait en dehors du cadre législatif, la confidentialité des données et leur persistance dans le temps. Hautement structurant, 91% des RSSI estiment que la sécurisation des données stockées dans le Cloud requiert des dispositifs caractéristiques.

Les pratiques des salariés alimentent aussi le risque, dont l'utilisation de terminaux personnels dans le cadre professionnel. En revanche la sensibilisation aux cyber-risques est en progression et plus de la moitié des entreprises (57%) a mis en place des procédures de vérification du respect des recommandations, in fine en hausse de 6%, 58% des RSSI attestent du bon respect des procédures.

Parmi les nouveaux usages du numérique, les objets connectés et le machine to machine (M2M), représentent un risque élevé.

**L'enjeu sur l'avenir est prioritairement humain.** Si les entreprises envisagent encore massivement d'investir dans l'acquisition de solutions techniques, près d'une sur deux prévoit d'augmenter les ressources humaines dédiées, souhaitant replacer la gouvernance de la cyber-sécurité au bon niveau et mieux former et sensibiliser les usagers pour mieux agir.

**Le « baromètre de la cyber-sécurité des entreprises »  
résultats détaillé du sondage OpinionWay pour le CESIN est disponible sur demande.**

## **A propos du CESIN**

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la sécurité de l'information et du numérique.

Le CESIN est un lieu d'échange de connaissances et d'expériences qui permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics.

Le Club conduit des ateliers et groupes de travail, mène des actions de sensibilisation et de conseil, organise des congrès, colloques, ou conférences.

Il participe à des démarches nationales dont l'objet est la promotion de la sécurité de l'information et du numérique. Il est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN réunit plus de 280 membres issus de tous secteurs d'activité publics et privés : des membres actifs, responsables de la sécurité de l'information dans leur organisation, des membres associés, représentants de diverses autorités en charge de Sécurité de l'Information au plan national, des juristes experts de la sécurité IT.

[www.cesin.fr](http://www.cesin.fr)