Communiqué de Presse

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

La 3ème édition du baromètre annuel du CESIN propose une analyse exclusive de la cybersécurité des grandes entreprises françaises

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

Paris, le 15 janvier 2018 – Afin de mieux cerner l'état de l'art et la perception de la cybersécurité et de ses enjeux au sein des grandes entreprises françaises, le CESIN publie la troisième édition de son baromètre annuel avec OpinionWay. Le Club dévoile aujourd'hui les résultats de cette enquête indépendante et exclusive menée auprès de ses membres, Responsables Sécurité des Systèmes d'Information (RSSI) des grands groupes français.

Le sondage OpinionWay pour le CESIN a ciblé 343 membres de l'association, et les résultats de l'étude portent sur un échantillon de 142 répondants. Ils mettent à jour la perception et la réalité de la cybersécurité, avec de nouvelles données sur l'impact de la transformation numérique des entreprises.

Quatre grandes thématiques sont étudiées : l'évolution des cyberattaques, l'efficacité des solutions techniques, les perspectives pour l'avenir avec les enjeux de la transformation numérique, et enfin le RGPD avec son impact sur la gouvernance cyber dans les entreprises.

Les cyberattaques progressent encore dans la hiérarchie des préoccupations des entreprises

Pratiquement toutes les entreprises sondées affirment avoir été attaquées une ou plusieurs fois (92 %). Depuis un an, une sur deux constate une augmentation de 48 % du nombre d'attaques et, pour le quart d'entre elles, des impacts sur le business ont été ressentis : arrêt de la production, indisponibilité significative du site internet, perte de chiffre d'affaire...

Cette année encore le Ransomware demeure l'attaque cyber la plus fréquente. 73 % des entreprises ont fait face à une ou plusieurs demandes de rançons. 38 % ont subi une fraude externe et 30 % un vol d'information. 25% ont été touchées par des attaques en déni de service et 16 % par une défiguration de site web. A noter que les attaques *WannaCry* et *NotPetya* ne sont pas citées dans l'étude car, si ces attaques ont en effet généré énormément d'activités de prévention pour l'ensemble des RSSI, très peu d'entreprises membres du CESIN ont été effectivement touchées. En revanche lorsqu'elles l'ont été, ce fut avec des conséquences importantes pour le business ou l'image. **En hausse, plus d'une entreprise sur deux est touchée par le social engineering et les vulnérabilités résiduelles permanentes.**

Face aux cyber-risques, le nombre de solutions techniques déployées reste élevé

Les entreprises implantent en moyenne une douzaine de solutions techniques. Globalement, les solutions de protection disponibles sur le marché sont jugées de plus en plus efficaces et cela tend encore à augmenter, mais elles restent perfectibles et ne sont toutefois pas totalement adaptées dans 22 % des cas aux besoins de l'entreprise, et dans 34 % des cas à la fréquence actuelle des attaques.

Au-delà des antivirus, tunnels VPN, mécanismes de filtrage web et solutions antiSPAM, **on note une forte montée des souscriptions aux cyber-assurances, 40 % ont déjà souscrit** (+14 points cette année), 15 % sont en cours et 22 % l'envisagent. Ces tendances devront être analysées de manière plus poussée mais les attaques précédemment citées ainsi que les conséquences de potentielles non-conformités au GDPR ne sont sans doute pas étrangères à ce phénomène.

Par ailleurs, l'entité jugée la plus légitime pour conseiller les entreprises sur la gestion des cyber-risques est l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), ce qui est le résultat de l'engagement de l'agence vers les secteurs hors OIV ou administrations depuis plusieurs années.

Dans ce contexte, la transformation numérique apporte elle aussi son lot de risques

La transformation numérique influence le niveau d'exposition au risque dans le cadre de la gestion des données.

Pour le Cloud, déjà très répandu dans les entreprises puisque 87 % d'entre elles y stockent des données notamment sous sa forme hybride public/privé, la problématique de la confidentialité des données représente l'enjeu principal en matière de cybersécurité. **94 % estiment que la sécurisation des données hébergées dans le Cloud nécessite des outils spécifiques.**

Les pratiques des salariés mettent aussi à mal la cybersécurité, notamment le Shadow IT. L'utilisation de terminaux multiples et l'usage personnel de ces derniers fournis par l'entreprise augmentent également significativement les risques.

Concernant l'internet des objets, les failles de sécurité de l'IoT sont le premier défi à relever en entreprise.

73 % des RSSI pensent que les salariés sont plutôt bien sensibilisés aux risques mais peu proactifs : 62 % des entreprises ont donc mis en place des procédures de vérification du respect des recommandations par les salariés.

La nouvelle réglementation relative à la protection des données personnelles complique la gestion des risques

Le RGPD grève les budgets avec un coût supplémentaire, mais ajoute également une charge de travail pour 89 % des RSSI. Ces derniers cumulent parfois la fonction de DPO, qui a priori ne s'avère pas incompatible avec le rôle de RSSI. Plus préoccupant, la majorité des entreprises sondées déclarent ne pas avoir achevé leurs chantiers de mise en conformité avec le RGPD et ne sont pas sûres de pouvoir les finaliser pour la date butoir du 25 mai 2018.

Le RGPD est cependant bien perçu par les entreprises, 83 % d'entre elles le considèrent comme un réel moyen de renforcer la protection des données.

Le processus de mise en conformité au RGPD a entraîné une évolution de la gouvernance des données

D'une part, la mise en conformité a déjà permis de refonder la gouvernance de la cybersécurité dans une entreprise sur deux. **71 % sont confiants sur la prise en compte des enjeux de la cybersécurité par le COMEX,** et 63 % pensent que leur entreprise à la capacité à faire face aux cyber-

risques. 81 % déclarent vouloir acquérir de nouvelles solutions techniques, 64 % envisagent d'augmenter les budgets alloués à la protection et 62 % projettent d'accroître les effectifs liés. Des investissements qui font écho à la faible part du budget IT actuellement consacré à la sécurité, soit **moins de 5 % pour 31 % des entreprises**.

D'autre part, pour 52 % des RSSI, la démarche de conformité au RGPD a déjà modifié la gouvernance de l'entreprise en matière de protection de l'information.

« baromètre annuel de la cybersécurité des entreprises »

« Enquête OpinionWay pour le CESIN réalisée en ligne du 21 novembre au 27 décembre 2017 auprès de 142 membres du CESIN ».

Retrouvez l'intégralité des résultats du sondage OpinionWay pour le CESIN . 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.

Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN est partenaire de plusieurs organismes et institutions, comme l'ANSSI, la CNIL, la BEFTI, la Gendarmerie Nationale, l'ARJEL, le Cercle Européen de la sécurité, l'AFAI, l'EBG, le CyberCercle ou encore l'EPITA.

Le CESIN compte plus de 350 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120.

www.cesin.fr