Communiqués de presse

Selon les résultats de l’étude C-Suite d’IBM : les dirigeants ne sont pas en phase avec les RSSI sur la façon de lutter contre les cybercriminels

Education et engagement sont nécessaires pour mettre les dirigeants au niveau du nouvel environnement de sécurité

Paris - 17 févr. 2016: La division sécurité d’IBM et l'Institut IBM for Business Value (IBV) publient aujourd'hui les résultats d’une étude réalisée auprès de plus de 700 dirigeants qui met en lumière leur confusion concernant leurs véritables ennemis cyber et la façon de les combattre efficacement.

La nouvelle étude, *Securing the C-Suite, Cybersecurity Perspectives from the Boardroom and C-Suite* est basée sur des entretiens avec des dirigeants de 28 pays et de 18 secteurs industriels concernant la cybersécurité dans l'entreprise. L’étude n’a pas pris en compte les responsables de la sécurité des systèmes d'information (RSSI), afin d’obtenir une image fidèle de ce que les dirigeants pensent de la cybersécurité. Si sur le papier, la cybersécurité est considérée comme une préoccupation majeure pour 68% des dirigeants1, et que 75% pensent qu’une stratégie globale de sécurité est importante, l'étude révèle que les dirigeants clés doivent être plus engagés auprès des RSSI, au-delà de la stratégie en matière de sécurité, et avoir un rôle plus actif.

L’une des principales conclusions de l'étude est que 70% des dirigeants pensent que les individus malveillants constituent la plus grande menace pour leur entreprise. Selon un rapport des Nations Unies2, la réalité est que 80% des cyberattaques sont réalisées par des réseaux criminels hautement organisés au sein desquels les données, les outils et l'expertise sont largement partagés. L'étude C-Suite révèle un large éventail d'ennemis : 54% des dirigeants reconnaissent que les réseaux criminels sont un sujet de préoccupation mais leur ont donné un poids à peu près égal aux individus malveillants (50%).

Plus de 50% des PDG s’accordent à dire qu’une collaboration est nécessaire pour lutter contre la cybercriminalité. Ironiquement, seulement 1/3 des chefs d'entreprise a exprimé sa volonté de partager à l'extérieur ses informations sur les incidents liés à la cybersécurité survenus dans leur entreprise. Cette situation est un frein à la collaboration coordonnée au niveau de l'industrie, alors même que les groupes de pirates partagent de mieux en mieux l'information en temps quasi réel sur le Dark Web. Les PDG soulignent également que les organisations externes doivent faire davantage ; une surveillance accrue du gouvernement, une augmentation de la collaboration dans l’industrie, un partage de l'information transfrontalière - cette dichotomie doit être résolue.

«Le monde de la cybercriminalité est en pleine évolution, mais de nombreux dirigeants n'ont pas mis à jour leur compréhension des menaces », **a déclaré Caleb Barlow, Vice-Président, IBM Security** *. « Bien que les RSSI et le Conseil d'administration puissent aider à fournir les conseils et des outils appropriés, les dirigeants en marketing, ressources humaines et finances, quelques-uns des départements les plus exposés et les plus fournis en données sensibles, devraient s'impliquer de façon plus proactive dans les décisions de sécurité avec les RSSI. »*

En fait, les départements marketing, ressources humaines, et finances représentent des cibles de choix pour les cybercriminels car ils gèrent les données clients et employés parmi les plus sensibles, avec les données financières de l'entreprise et les informations bancaires. Dans l'étude, environ 60% des directeurs financiers, DRH, et directeurs marketing reconnaissent volontiers qu'ils, et par extension leurs divisions, ne sont pas actifs dans la stratégie et l'exécution de la politique de cybersécurité de l'entreprise. Par exemple, seuls 57% des DRH ont déployé une formation à la cybersécurité pour les employés, première étape pour que ces derniers s'engagent en la matière.

Que peuvent faire les entreprises ?

Un nombre impressionnant de dirigeants interrogés, 94%, pensent qu'il y a une certaine probabilité pour que leur entreprise subisse un incident de cybersécurité significatif au cours des deux prochaines années. Selon l'étude d'IBM, 17% des personnes interrogées se sentent capables et prêtes à répondre à ces menaces. IBM a identifié des répondants exceptionnels, 17% de répondants classés «Cyber-Securisés», ce sont les dirigeants les plus préparés et capables de faire face aux menaces. Les dirigeants « Cyber sécurisés » sont deux fois plus susceptibles d'avoir intégré la collaboration dans leur politique de cybersécurité et deux fois plus susceptibles d'avoir intégré la cybersécurité à l'ordre du jour des Conseils d'administration de façon régulière.

Conseils "Cyber-Securisés» pour les entreprises :

• **Comprendre le risque :** Évaluer les risques liés à votre écosystème, analyser les risques de sécurité, développer l'éducation et la formation des employés et intégrer la sécurité dans la stratégie de risques de l'entreprise.

• **Collaborer, éduquer et responsabiliser :** Mettre en place un programme de gouvernance de la sécurité,

accroître le pouvoir des RSSI, promouvoir et discuter régulièrement de la cybersécurité lors des réunions de direction, intégrer les dirigeants dans l'élaboration d'une stratégie de réponse aux incidents.

• **Gérer les risques avec vigilance et rapidité** : Mettre en œuvre une surveillance continue de la sécurité, tirer profit des analyses d'incidents, partager et utiliser les renseignements de sécurité pour sécuriser l'environnement, comprendre où les données numériques des entreprises se trouvent et élaborer des stratégies en conséquence, développer et appliquer les politiques de cybersécurité.

Pour télécharger le rapport complet et l'infographie : **ibm.com/security/ciso**.

A propos d'IBM Security

La plateforme de sécurité IBM apporte les renseignements de sécurité pour aider les organisations à protéger les personnes, les données, les applications et les infrastructures. Les solutions IBM couvrent la gestion des identités et des accès, le SIEM (Security Information and Event Management), la sécurité des données, la sécurité des applications, la gestion du risque, la gestion des terminaux, la nouvelle génération de protection contre les intrusions et d'autres sujets. IBM dispose d'une des plus importantes organisations au monde de recherche et développement et de prestations de services dans le domaine de la sécurité.

Pour plus d'informations : www.ibm.com/security/fr/fr

Blog US : www.securityintelligence.com

Suivez notre actualité sur Twitter @IBMSecurityFR

- "Redefining Boundaries: Insights from the Global C-suite Study." IBM Institute for Business Value. November 2015. http://www-935.ibm.com/services/c-suite/study/study/
- UNODC Comprehensive Study on Cybercrime 2013