# Qui est responsable de la cybersécurité : le RSSI, le DSI, le PDG ou vous ? | Le Net Expert Informatique

**La menace informatique est changeante et les décideurs IT peinent à s'adapter à un danger croissant. La cybermenace, certes significative, ne constitue qu'un élément de la sécurité de l'entreprise. Dès lors, qui devrait être responsable de la sécurité et comment les entreprises peuvent adopter une approche plus proactive face aux menaces ? Cinq experts IT donnent leur avis.**

**1. Faites de la sécurité la responsabilité de tous les salariés**

« Le directeur général, et n'importe qui d'autre » répond David Allison à la question de savoir qui est responsable de la sécurité au sein de l'entreprise. Le responsable des systèmes métier pour Aggregate Industries estime que le PDG devrait être responsable de la sécurité, mais que chaque salarié a une responsabilité personnelle.

« La sécurité, ce n'est pas le confinement et la prévention » juge Allison, même si les pare-feu, les antivirus et les autres mesures IT doivent être considérés comme acquis. « Une grande sécurité, c'est affaire d'éducation, de sensibilisation et de responsabilité individuelle. »

Pour lui, le dirigeant de l'entreprise doit s'engager personnellement pour disposer d'une équipe en place formant le personnel dans un large éventail de domaines comme la gestion des courriels, la détection des liens suspects et l'adoption de bonnes pratiques pour les mots de passe.

« La sécurité a besoin d'être une culture diffusée au sein de l'organisation » souligne David Allison. « Le PDG met en place cette culture. Le responsable de la sécurité informatique (RSSI) définit et exécute la stratégie répondant à ce besoin – et chaque salarié est responsable de s'assurer d'adopter et de suivre les pratiques requises. »

**2. Ne vous reposez pas sur des produits technologiques**

Tim Holman, le président de l'ISSA, une association britannique de sécurité des SI, estime que la responsabilité au sein d'une entreprise se situe toujours au niveau des propriétaires ou des comités de direction. Certains Comex peuvent désigner un DSI, RSSI ou un directeur IT comme le responsable de la sécurité, mais ces individus ne peuvent jamais être tenus pour responsables.

« Les entreprises doivent avoir conscience de l'ampleur de la menace lorsqu'elles font du commerce sur Internet ou stockent leurs données sur le Cloud » déclare Holman. « Les entreprises peuvent charger un DSI d'implémenter une solution Cloud, mais elles resteront toujours responsables si quelque chose tourne mal. »

Face aux cybermenaces, les firmes doivent adopter une attitude proactive, et elles peuvent le faire au travers d'une simple analyse de risques, ou en suivant des standards comme IASME ou Cyber Essentials. D'après Tim Holman, la compréhension des enjeux liés à la sécurité progresse en consacrant du temps avec des dirigeants et en leur expliquant en termes simples les risques inhérents au business en ligne.

« La cybermenace ne peut pas être résolue en achetant des produits. Une approche de bon sens consistant à réduire le volume de données sensibles stockées, à éjecter les fournisseurs non-sécurisés, à restreindre l'accès aux données et à souscrire une cyber-couverture sera souvent dix fois plus efficace et dix fois moins chère que la dernière génération d'appliance de sécurité vendue par les experts de la vente. »

**3- Gardez sous contrôle les périls des terminaux mobiles**

David Reed, directeur des services d'information et de l'infrastructure à la Press Association (PA), juge complexe la discussion autour de la sécurité, mais est d'avis que la responsabilité commence au sommet de l'IT. « Si en tant que DSI, vous n'êtes pas en mesure de percevoir les dangers liés à la sécurité, vous ne faites pas un assez bon travail » tranche-t-il.

Un des domaines les plus importants pour Press Association est ainsi la gestion du mobile. Les journalistes de la société ont à traiter des informations extrêmement sensibles, et la menace de piratage d'un terminal, bien que sérieuse, n'est pas aussi répandue qu'une simple perte ou un vol. PA travaille avec EE pour implémenter une stratégie mobile COPE (un terminal de l'entreprise pour un usage personnel et professionnel) utilisant des Samsung S4 Mini et le système de sécurité Knox.

« Un conteneur peut être créé sur chacun des téléphones pour stocker séparément documents de travail, courriels et contacts et éléments personnels. Nos journalistes disposent principalement de deux zones sur leurs téléphones : une pour l'usage personnel et l'autre pour le travail » précise David Reed.

« Chez PA, nous aidons les journalistes en recommandant des apps. Nous avons appliqué ce principe pour les jeux du Commonwealth de 2014 en envoyant aux journalistes présents sur l'évènement un message pour télécharger l'app Team GB. L'appli était en liste blanche et installée simplement dans le conteneur. »

**4- Obtenez le soutien du dirigeant pour les démarches de gouvernance**

Pour Omid Shiraji, ex-DSI de Working Links, la responsabilité de la sécurité est totalement liée à l'entreprise et à la nature de ses activités. Il n'est pas persuadé de la nécessité de disposer d'un RSSI dans la majorité des organisations.

« La sécurité IT est une commodité. Vous pouvez acheter des produits et de l'expertise auprès d'un fournisseur » juge-t-il. « La même chose est vraie en ce qui concerne la sécurité des entreprises dans de nombreux cas – les processus et la gouvernance sont une marchandise que vous pouvez acheter comme un service géré. »

Omid Shiraji préférerait consacrer son budget IT limité aux opérations en première ligne, et ensuite s'appuyer sur une expertise spécifique pour l'aider à protéger ses données et guider son personnel. La société a récemment été certifiée ISO 27001 et le support du PDG s'est révélé essentiel.

« Les individus changent leur comportement car ils entendent le PDG parler des conséquences majeures des activités non protégées » déclare-t-il. « La sécurité IT est en fait le travail de chaque employé, mais le patron doit soutenir chaque initiative en matière de sécurité et de gouvernance dans l'entreprise. Et c'est ce qui s'est passé chez Working Links. »

**5. Créez une culture du risque pragmatique**

Julian Self, un DSI expérimenté qui a travaillé pour de nombreux acteurs de la finance, fait lui une analyse différente et estime que l'importance du RSSI dans l'entreprise continue de grandir. Selon lui, il est du ressort du DSI de promouvoir auprès des dirigeants les avantages d'un spécialiste de la sécurité.

« Dans un monde déjà hyper-connecté, et avec l'avènement de l'Internet des Objets, le travail de sécurisation des données de l'entreprise devient infiniment plus complexe avec des flux de données qui entrent et sortent de nombreux terminaux » commente Julian Self, pour qui le panorama de la menace continue d'évoluer.

« Les RSSI ne réussiront pas à moins d'avoir l'adhésion et l'engagement des métiers. Sans cela, ils seront simplement perçus comme des freins à l'activité et leurs efforts seront contournés. »

« Fondamentalement, les RSSI ont besoin de créer une prise de conscience et une culture pragmatique du risque afin que la sécurité de l'information soit appliquée de façon inconsciente dans tous les domaines de l'entreprise. Cette approche doit aller de pair avec une réponse à incidents qui soit proportionnée et sans alarmisme, et la gestion et la réaction au risque, restaurant in fine la confiance de l'entreprise. »

---



---



Source : http://www.zdnet.fr/actualites/qui-est-responsable-de-la-cybersecurite-le-rssi-le-dsi-le-pdg-ou-vous-39826198.htm