IT-expert Magazine Sécurité : Oui, il faut « oser dire non » mais… » IT-expert Magazine

La communauté sécurité est actuellement en plein émoi suite au discours de Patrick Pailloux, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), lors des Assises de la Sécurité qui se sont tenues la semaine dernière. Au cœur de son intervention, un message : « osez dire non ». Savoir dire non quand les risques sont trop grands, quand les innovations peuvent être désastreuses ou encore quand les projets font perdre le contrôle sur le système d'information.

L'intégralité du discours se trouve ici http://www.ssi.gouv.fr/fr/anssi/publications/discours-de-patrick-pailloux-directeur-general-de-l-agence-nationale-de-la.html, il mérite d'être lu avec attention.

Il a reçu un accueil partagé dans la communauté sécurité. Sans rentrer dans une polémique stérile, je voudrais revenir sur le cœur du message et le mettre en relief des retours d'expérience que nous vivons au quotidien.

« Oser dire non », d'accord mais qui peut le faire ?

Le RSSI est positionné dans l'entreprise comme un conseil, un responsable de l'évaluation des risques avec un pouvoir d'alerte. Même si le RSSI est persuadé que des risques importants sont en train d'être pris, c'est bien au métier qu'il revient d'arbitrer. Le métier est avant tout motivé par la flexibilité, la rapidité, la souplesse, le retour sur investissement… Alors le RSSI explique, sensibilise et parfois il tente de dire non. Cependant un RSSI qui dit non, aujourd'hui c'est un RSSI contourné sans aucune vergogne. Et, souvent, malheureusement, sans autre réaction du management que « ça se passera mieux la prochaine fois »…

J'ai rencontré cette situation trop souvent pour croire que tous les RSSI ont le pouvoir de dire non. Et c'est bien là le cœur du problème. Dans la logique d'acceptation des risques, ce n'est pas au RSSI de dire non, c'est bien aux dirigeants de l'entreprise ou à la DSI. Ce point a d'ailleurs été mentionné lors de la conférence des Assises. Et Patrick Pailloux l'a bien explicité : les dirigeants doivent montrer l'exemple. Aujourd'hui ce n'est pas le cas, loin de là. Les principales exceptions sécurité sont justement réalisées pour les fameux « VIP ». Pourtant alertés sur la valeur des informations qu'ils manipulent, ils sont souvent très peu conscients qu'un incident peut se produire brutalement, sans alerte préalable et avoir des conséquences graves. Les messages de sensibilisation du RSSI sont écoutés, mais semblent souvent trop lointains pour éveiller une réelle prise de conscience (étude catastrophiste avec des montants faramineux, chiffres en provenance des États-Unis…).

« Oser dire non », d'accord mais avec quels arguments ?

IT-expert Magazine Sécurité : Oui, il faut « oser dire non » mais… » IT-expert Magazine

Il faut à mon sens oser parler de sécurité, avec les métiers, avec les dirigeants, mais pas à mots couverts, trop théoriques. Il faut détailler des cas concrets, proches, qui permettent de concrétiser les risques. Nos expériences le montrent, quand un incident a touché une organisation française, lorsque des impacts ont pu être évalués, l'attention des métiers et des dirigeants augmente largement.

Imaginons un instant avoir des éléments tels que « 15 incidents majeurs entraînant une fuite de données stratégiques ont eu lieu dans le secteur de l'énergie en France » ou encore « Lors des 6 derniers mois, les intrusions ont majoritairement eu lieu du fait de l'utilisation de postes personnels de collaborateurs ».

Alors là oui, le RSSI disposerait de vrais arguments, résonnant aux oreilles des dirigeants pour expliquer pourquoi telle ou telle pratique est dangereuse. De plus, cela permettrait d'amener du recul dans les analyses de risques souvent réalisées « à dire d'expert » par manque d'historiques ou de statistiques sur les incidents.

Dans cette logique, l'ANSSI peut jouer un rôle déterminant, en faisant part des multiples retours d'expériences dont elle dispose à la communauté sécurité mais aussi, et surtout, aux dirigeants des grandes entreprises et administrations, dans un discours simple, clair et mobilisateur comme elle sait très bien le faire lors des Assises !

Tribune par Gérôme BILLOIS, manager au sein de la Practice Sécurité & Risk Management de Solucom