Tenacy

RSSI

10 conseils pour vous faire entendre en entreprise

Chez Tenacy, on sait combien les RSSI ont parfois du mal à faire entendre leur voix, que ce soit auprès de leur direction ou de leurs collaborateurs. On a donc créé une infographie rassemblant tout plein de conseils pour les (vous) y aider.

Bonne lecture !

Se faire entendre par sa direction

1 Parlez risque

La direction comprend mieux le langage du risque que celui de la technique.

Transformez les menaces abstraites en risques concrets pour l'entreprise : perte de données, dommages à la réputation, interruption d'activité…

Vous pouvez vous appuyer sur :

- des **exemples d'autres entreprises** du même secteur que vous qui ont subi des cyberattaques
- des **scénarios crédibles** décrivant les conséquences d'un incident dans votre entreprise

2 Parlez business

Un argument qui fait souvent mouche : **la cybersécurité peut être un avantage concurrentiel** ! Appliquer des normes de sécurité élevées (et le justifier via des certifications) **rassure les clients et partenaires**.

Pensez aussi à l'**aspect budgétaire**. On a justement créé une infographie chiffrée et sourcée pour leur démontrer que se faire attaquer coûte bien plus cher que se protéger !

3 Parlez performance

Créez des **tableaux de bord de sécurité** clairs et accessibles, qui reprennent certains KPI essentiels :

- **nombre d'incidents évités,**
- **nombre de failles détectées,**
- **pourcentage de collaborateurs formés à la cyber…**

C'est le meilleur moyen de **démontrer que vos actions donnent des résultats con-crets** et que vous ne jetez pas l'argent par les fenêtres.

4 Parlez stratégie

Organisez des ateliers pour **former et informer les membres du COMEX**. Si la direction se sent impliquée dans les décisions et la stratégie cyber, il y a plus de chances qu'elle se montre de bonne volonté quand vient l'heure des budgets…

Présentez-leur aussi votre **plan de gestion de crise** : cela permet de les rassurer et de les préparer, tout en mettant en valeur votre expertise. Ça ne mange pas de pain, et c'est toujours efficace.

5 Pensez communication

Comme dans toute relation, l'important est de co-mmu-ni-quer !

Misez sur la transparence, avec des **rapports** réguliers et l'instauration d'un réel dialogue avec votre direction : enjeux métiers, innovations de l'entreprise, compromis à faire… Démontrez votre bonne volonté et votre **compréhension du contexte de l'entreprise**.

Se faire entendre par ses collaborateurs

6 Soyez simple

Non, vos collaborateurs ne sont pas des pros de la cyber (et vous le constatez sûrement déjà). Alors pas la peine de leur parler d'endpoint, de RGS ou de SOC : allez à l'essentiel ! **Expliquez-leur ce qui les concerne**, les pratiques et les risques du quotidien – et pas toute la machinerie qu'il y a derrière.

Pour vos collègues les plus curieux, qui veulent connaître le pourquoi du comment, n'hésitez pas à les renvoyer vers des ressources dédiées aux cyber-novices (par exemple le MOOC SecNumacadémie proposé par l'ANSSI).

7 Soyez sympa

On sait que ce n'est pas toujours facile, mais essayez de faire preuve d'**indulgence** et de **proximité** avec vos collaborateurs. Si vous êtes perçu comme strict ou inaccessible, ils risquent de se détourner des règles de sécurité ou – pire – de ne pas signaler des incidents potentiels.

D'ailleurs, quand un incident se produit via un collaborateur, **évitez de le culpabiliser** : préférez une approche pédagogique, pour que cette mauvaise expérience devienne constructive. Cela incite les collaborateurs à déclarer leurs erreurs sans craindre d'être sanctionnés.

L'**écoute** est aussi une qualité importante : organisez des rencontres régulières pour prendre le pouls des équipes et comprendre leurs préoccupations.

8 Soyez pédagogue

Faites de vos sessions de formation des moments conviviaux en misant sur les serious games, les vidéos, les quiz (avec des récompenses à la clé, ça marche toujours)…

N'oubliez pas d'**adapter le niveau de détail et d'exigence** au niveau de sensibilisation nécessaire de chaque service : entre le personnel technique et les RH, les risques ne sont pas les mêmes.

9 Soyez concret

Faites comprendre à vos collègues que la cybersécurité les concerne tous, en expliquant les conséquences directes de certains comportements et mauvaises pratiques :

- cliquer sur n'importe quel lien → introduction d'un virus dans l'ordinateur
- laisser son ordinateur sans surveillance → vol de données…

C'est bien connu : les petits ruisseaux font les grandes rivières !

10 Soyez un modèle

Être respecté et écouté implique d'**être irréprochable sur vos propres pratiques de sécurité**. Le « faites ce que je dis, pas ce que je fais » risque d'en agacer plus d'un…

Vous pouvez (et devez) aussi **mettre en valeur les collaborateurs modèles**, qui mettent en œuvre les bonnes pratiques cyber sans broncher. Félicitations durant une réunion d'équipe, message sur un canal de messagerie, cadeaux – encore une fois, les récompenses, ça marche toujours…

Voilà, vous avez en main plein d'outils pour mieux vous faire entendre dans votre organisation !

Mais il y en a un qu'on ne vous a pas encore présenté…

Cliquez ici pour le découvrir