Testez le niveau de vulnérabilité de votre organisation

L'objectif de ce Quizz est de mesurer les failles potentielles de sécurité pouvant entrainer une attaque informatique sur votre réseau d'entreprise / collectivité.
L'ensemble des points ci-dessous sont considérés comment étant des catalyseurs de cybercriminalité.

Si vous n'avez pas connaissance d'un des points mentionnés, répondez « non » ; en cybersécurité, l'inconnu est synonyme de risque.

BONNES PRATIQUES	Oui	Partiellement	Non
Les collaborateurs utilisent des mots de passe suivant une politique complexe mise en place dans l'entreprise (chiffres, lettres minuscules, majuscules, caractères spéciaux, 10 caractères,...)	☐	☐	☐
Les collaborateurs se connectent depuis l'extérieur au réseau de l'entreprise de façon sécurisée	☐	☐	☐
Vos données de production sont sauvegardées quotidiennement ; il est possible de les récupérer à tout moment	☐	☐	☐
Votre Système d'Information est supervisé permettant ainsi de prévenir les incidents de sécurité	☐	☐	☐
Il est impossible pour les salariés de se connecter au réseau informatique de l'entreprise avec leurs propres outils (clé USB, smartphone, tablette, PC portable personnel, ...)	☐	☐	☐
Les collaborateurs ne peuvent pas installer d'applications sur leur poste de travail, ils ont besoin de l'autorisation technique du SI	☐	☐	☐
Les collaborateurs ne peuvent pas se connecter sur plusieurs sessions Windows en même temps. Des règles permettent de verrouiller automatiquement une session en cas d'inactivité prolongée	☐	☐	☐

HUMAIN	Oui	Partiellement	Non
Les collaborateurs sont sensibilisés à la sécurité informatique	☐	☐	☐
Votre entreprise n'a jamais subi, selon vous, une attaque informatique ou une malveillance	☐	☐	☐
Les collaborateurs ont signé une charte informatique qui règlemente l'usage des systèmes de l'entreprise	☐	☐	☐
La politique RH est synchronisée avec la politique SI de l'entreprise pour permettre la fermeture des différents comptes utilisateurs lors du départ d'un employé	☐	☐	☐

RGPD	Oui	Partiellement	Non
Un DPO (Data Protection Officer) a été nommé au sein de votre organisation	☐	☐	☐
Un processus de vérification de l'intégrité et de protection des données personnelles a été initié	☐	☐	☐
Des règles de classification de l'information sont en place au sein de mon organisation afin que seules les personnes destinées à manipuler certains type de données y aient accès	☐	☐	☐
Mon entreprise est sensibilisée sur les impacts en cas de fuite de données personnelles et de non respect du Règlement Général de Protection des Données à caractère personnel	☐	☐	☐

ORGANISATIONNEL	Oui	Partiellement	Non
Mon réseau informatique est maintenu et les matériels sont sous contrat de service stipulant clairement les niveaux de services et les garanties	☐	☐	☐
Des audits de sécurité ont lieu régulièrement sur mon infrastructure	☐	☐	☐
Les droits informatiques des utilisateurs sont correctement gérés	☐	☐	☐
Une procédure de gestion de crise en cas d'attaque informatique a été formalisée	☐	☐	☐
Si vos données sont sauvegardés dans le Cloud, l'entreprise qui les héberge est basée en France	☐	☐	☐
En cas de perte ou de vol d'un équipement informatique, vous disposez de procédures et d'outils pour en verrouiller le contenu et limiter l'accès au système informatique de l'entreprise	☐	☐	☐
Votre entreprise dispose d'un accès à internet filtré dont l'accès à certains sites est restreint (Facebook, vente-privée, ...)	☐	☐	☐
Si vous disposez d'un réseau wifi pour vos collaborateurs ou vos invités, cet accès est protégé par un mot de passe dit "fort"	☐	☐	☐
Vos emails sont sauvegardés	☐	☐	☐
Vous recevez peu, voire pas de SPAM, ou de courriers indésirables	☐	☐	☐
Un antivirus est installé sur l'ensemble des postes informatiques	☐	☐	☐
Nombre de cases cochées	☐	☐	☐

Total des points : [..... (nombre **Oui**) x 0] + [..... (nombre **Partiellement**) x 1] + [..... (nombre **Non**) x 2] = ...

SYSCOM Groupe SCOPELEC

Analyse des risques

Vous comptez plus de 35 points :

FRAGILITE !

Pas de panique, mais prenons conscience ensemble qu'il faudra changer les choses. La cybersécurité n'est pas actuellement un sujet pour votre entreprise, mais dans le monde d'aujourd'hui, il va falloir que ça le devienne. Un audit sécurité semble obligatoire pour faire un point plus précis sur les failles techniques de votre infrastructure informatique. Il y a ensuite des "Quick Win" vous permettant de résoudre certaines de ces failles rapidement et à moindre coût. Le tout doit pouvoir s'envisager dans une politique globale et un plan de mise en conformité sur le long terme que nous pouvons définir ensemble.

Vous comptez entre 20 et 35 points :

LES BASES SONT LA ...

Respirez, les outils déjà mis en place ont peut être déjà montré leur efficacité. En effet, même si ce n'est pas une priorité pour vous, la cybersécurité reste un sujet qui suscite votre attention. Votre protection en surface semble satisfaisante et vous protège ainsi contre les attaques connues. Et les attaques inconnues alors, celles dont nous n'avons pas encore entendu parler. Ces petits malwares qui sont peut-être déjà cachés dans votre réseau, endormis, n'attendant qu'un signal pour vous infecter. Et les risques internes, ceux qui se trouvent entre le clavier et la chaise de l'utilisateur ? Peut-être qu'un rappel des bonnes pratiques informatiques serait une bonne base pour diminuer ces risques là, en effet un utilisateur bien informé, c'est 90% de risques en moins. Quand aux petits malwares ou aux attaques inconnues, appelées "ZeroDay", nous pouvons les détecter avec nos outils comportementaux basés sur l'intelligence artificielle. Alors, un petit scan de vulnérabilité pour regarder tout ça ?

Vous comptez moins de 20 points :

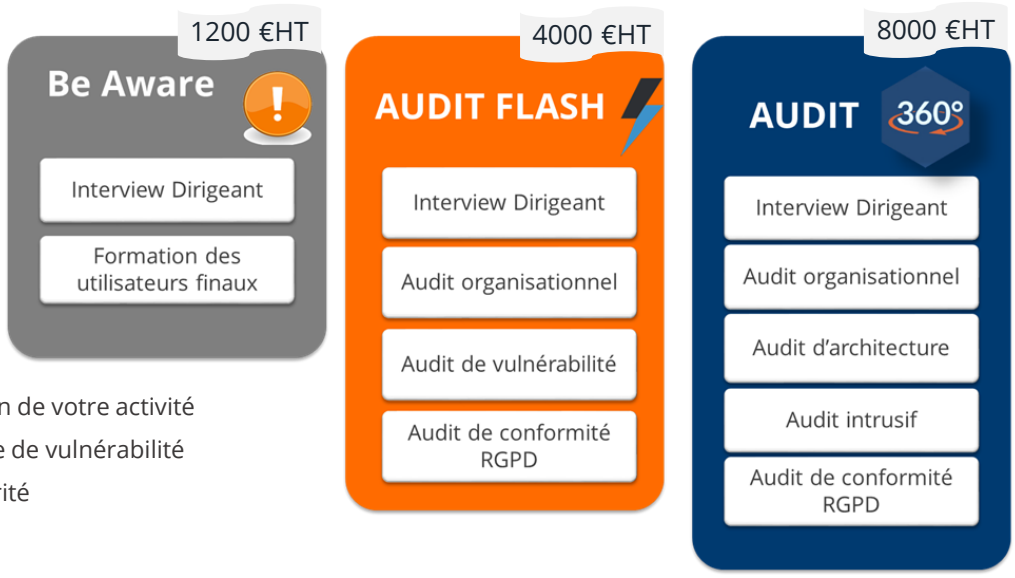
SOYONS PERFECTIONNISTES...

Un sujet majeur pour vous. Passons donc l'étape de sensibilisation qui n'est plus à faire. Par contre, qu'en est-il de vos collaborateurs ? Pour aller plus loin, la surveillance continue de votre infrastructure réseau semble pour vous primordiale. Un SOC, Sécurity Operating Center est la solution. Trop cher ? Pas avec Exzo Guard. Notre offre, résolument tournée vers les TPE/PME se veut plus accessible et doit pouvoir vous permettre de suivre les évolutions de votre réseau et les éventuelles failles de sécurité associées. Mais avant de mettre en place cela, vérifions l'état actuel de votre réseau et la conformité à la RGPD par un Audit Pentesting qui va mettre à l'épreuve votre réseau et vérifier que l'on ne puisse pas accéder à vos données et les récupérer.

La solution Exzo Guard

Une approche à 360°

EXZO GUARD by SYSCOM est une **méthode de sécurité globale** destinée aussi bien aux PME, qu'aux collectivités.



- ✓ 3 approches progressives en fonction de votre activité
- ✓ Automatisez vos processus d'analyse de vulnérabilité
- ✓ Surveillance 24/7 des failles de sécurité
- ✓ Mise en conformité RGPD

Je suis intéressé par : ☐ Audit 360° ☐ Audit Flash ☐ Journée de sensibilisation (Be Aware)

Nom et prénom ou Raison sociale	
Représenté par	
Rue ou Boîte Postale	
Code Postal / Commune	
SIRET	
Téléphone / Fax	
Email	
Mobile	

Signature et Tampon Client

N° Vert : **0800 800 990**
commercial@groupe-scopelec.fr