Conseils de Cybersécurité

Nom de l'entreprise: Test tb SARL

Question 1: Combien d'ordinateurs et de périphériques connectés utilisez-vous dans votre entreprise ?

Réponse: 0-10

Conseil: Avec 0-10 appareils connectés, voici 3 conseils pour renforcer votre cybersécurité :

1. Mettez à jour régulièrement vos systèmes d'exploitation et vos applications pour combler les failles.

2. Utilisez des solutions antivirus et antimalware pour détecter et bloquer les menaces potentielles.

3. Sensibilisez et formez votre personnel aux bonnes pratiques de sécurité, comme la gestion des mots de passe.

Question 2: Vos données sont-elles stockées localement sur des serveurs ou dans le cloud ?

Réponse: cloud

Conseil: 1. Utilisez une authentification à facteurs multiples pour renforcer l'accès à vos données sensibles.

2. Chiffrez vos données avant de les stocker sur le cloud pour assurer leur confidentialité.

3. Assurez-vous que votre fournisseur de services cloud dispose de normes de sécurité et de conformité fiables.

Question 3: Comment les données sont-elles partagées au sein de votre entreprise?

Conseils de Cybersécurité

Réponse: interne

Conseil: Pour sécuriser le partage de données sur votre réseau interne, voici deux conseils :

1. Mettez en place des règles strictes d'accès aux données en utilisant des autorisations basées sur les rôles.
2. Chiffrez les données sensibles lors de leur transfert sur le réseau pour éviter les interceptions malveillantes.

Question 4: Quels types de logiciels utilisez-vous pour la gestion de votre entreprise?

Réponse: ['comptabilité', 'crm', '']

Conseil: Pour les logiciels de comptabilité :

- Assurez-vous de mettre à jour régulièrement le logiciel pour combler les failles de sécurité.
- Limitez l'accès aux informations sensibles en ne donnant les droits qu'aux personnes nécessaires.

Pour les logiciels CRM :

- Utilisez des mots de passe forts et encouragez la double authentification pour protéger les données.
- Sensibilisez régulièrement les utilisateurs aux risques de sécurité et aux bonnes pratiques à adopter.

Question 5: Offrez-vous des formations et/ou des séances de sensibilisations à la cybersécurité à vos employés ? Si oui, à quelle fréquence ?

Réponse: non

Conseils de Cybersécurité

Conseil: La formation en cybersécurité est essentielle pour prévenir les cyberattaques. Investissez-y régulièrement.

Conseil : Formez vos employés annuellement pour renforcer la sécurité de l'entreprise.

Question 6: Quels sont les réseaux sociaux que vous utilisez dans un cadre professionnel ?

Réponse: ['twitter', 'instagram', '']

Conseil: Sur Twitter et Instagram, il existe plusieurs risques liés à la cybersécurité, notamment :

1. Phishing : Les attaques de phishing sur Twitter et Instagram peuvent prendre la forme de messages directs ou de commentaires contenant des liens malveillants. Ces liens peuvent rediriger vers des sites frauduleux conçus pour voler vos informations personnelles.

2. Hameçonnage (phishing) : Les cybercriminels peuvent se faire passer pour des personnes ou des organisations légitimes afin de vous inciter à divulguer des informations sensibles telles que vos identifiants de connexion, mots de passe ou informations bancaires.

3. Ingénierie sociale (social engineering) : L'ingénierie sociale est une technique utilisée pour manipuler les individus afin d'obtenir des informations confidentielles. Par exemple, un attaquant peut prétendre être un employé de votre entreprise sur Twitter ou Instagram pour vous inciter à partager des informations sensibles.

Il est essentiel de sensibiliser vos collaborateurs à ces risques et de mettre en place des mesures de sécurité telles que l'authentification à deux facteurs, l'utilisation de mots de passe forts et la

vérification systématique de l'identité des personnes avec lesquelles vous communiquez en ligne.

Enfin, je vous recommande d'être vigilant et de ne jamais partager d'informations sensibles ou personnelles sur les réseaux sociaux sans être sûr de l'identité de la personne avec laquelle vous communiquez.

Question 7: Quels outils de sécurité utilisez-vous ?

Réponse: ['vpn']

Conseil: Vous devriez considérer en priorité : antivirus, pare-feu, gestionnaire de mot de passe et système de sauvegarde.

Ces outils sont prioritaires car ils couvrent différents aspects de la cybersécurité : l'antivirus protège contre les logiciels malveillants, le pare-feu sécurise le réseau, le gestionnaire de mot de passe renforce l'authentification et le système de sauvegarde permet de récupérer les données en cas de sinistre.

Question 8: Comment votre réseau wifi est-il accessible ?

Réponse: un mot de passe simple (123456789)

Conseil: Non, un mot de passe simple comme "123456789" n'est pas sécurisé. Utilisez plutôt une passphrase, c'est-à-dire une phrase longue et complexe. Par exemple : "LaPluieEnMarsEstToujoursBienvenue!". Les risques d'un réseau wifi mal sécurisé sont les intrusions, l'espionnage des données et les menaces malveillantes.

Conseils de Cybersécurité

Question 9: Quelles sont les actions que vous avez entrepris après une cyberattaque ? (Dans le cas où vous n?avez pas subi de cyber attaque, veuillez répondre comme si cela l?était)

Réponse: ['débranchement des machines', ' contact office fédérale de la cyber-sécurité']

Conseil: Pour être plus efficace lors d'une cyberattaque, vous pourriez également envisager de restreindre l'accès au réseau, de collecter des preuves pour soutenir l'enquête, de communiquer avec les parties prenantes internes et externes, de mettre en place des systèmes de sauvegarde et de restauration des données, et de former le personnel sur la gestion des cyberattaques.

Explication: Un plan d'urgence en cas de cyberattaque est essentiel pour réagir rapidement et efficacement pour limiter les dommages potentiels, protéger les données sensibles, et assurer la continuité des activités de l'organisation. Avoir un plan préétabli permet une réponse coordonnée et organisée, minimisant ainsi l'impact de l'attaque.

Question 10: Quel est votre domaine d?activité ?

Réponse: Boucherie

Conseil: 1. "Une boucherie a été victime d'une attaque de ransomware, bloquant l'accès à toutes leurs données clients et financières."

2. "Une autre boucherie a subi une intrusion de leur système de caisse, compromettant les informations de paiement des clients."

3. "Une attaque par phishing a touché une boucherie, où les employés ont été trompés pour divulguer des informations sensibles."