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: Pour sécuriser vos 0-10 ordinateurs et périphériques :

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

2. Utilisez des mots de passe robustes et différents pour chaque appareil afin de renforcer la sécurité.

3. Installez un antivirus et un pare-feu sur tous les appareils pour protéger contre les menaces potentielles.

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

Réponse: cloud

Conseil: 1. Assurez-vous d'utiliser des services cloud réputés et sécurisés pour stocker vos données sensibles.

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

3. Mettez en place une authentification forte pour limiter l'accès aux données stockées sur le cloud.

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

Réponse: interne

Conseils de Cybersécurité

Conseil: Pour sécuriser le partage de données sur votre réseau interne, je vous recommande :

1. Mettez en place des règles strictes d'accès aux données en fonction des niveaux de permissions des utilisateurs.
2. Chiffrez les données sensibles lors de leur transmission sur le réseau pour éviter toute interception malveillante.

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

Réponse: ['comptabilité', 'crm', '']

Conseil: Pour les logiciels de comptabilité : Effectuez des sauvegardes régulières des données sensibles, et mettez à jour le logiciel fréquemment.

Pour les logiciels CRM : Limitez l'accès aux informations sensibles en configurant correctement les autorisations des utilisateurs. Mettez à jour régulièrement le logiciel pour combler les failles de sécurité.

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

Conseil: La formation en cybersécurité est cruciale pour sensibiliser et prévenir les risques. Formez-les dès maintenant.

Conseil : Priorisez la formation en cybersécurité pour tous les employés chaque année.

Conseils de Cybersécurité

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

Réponse: ['twitter', 'instagram', '']

Conseil: Sur Twitter, vous pourriez être exposé à des risques tels que la diffusion de faux concours, l'hameçonnage (phishing) via des liens malveillants, l'usurpation d'identité pour des tentatives de fraude ou encore la diffusion de fausses informations pouvant nuire à votre réputation.

Sur Instagram, les risques incluent le cyberharcèlement, le vol d'identité pour la création de faux comptes, l'exposition à des contenus inappropriés ou encore la compromission de données personnelles via des messages directs frauduleux.

Il est essentiel de rester vigilant et de sensibiliser votre équipe sur les risques liés au social engineering, qui consiste à manipuler les individus pour obtenir des informations confidentielles. Par exemple, sur Twitter, un cybercriminel pourrait se faire passer pour un employé de votre entreprise et demander à un employé de divulguer des informations sensibles. Restez donc prudent et assurez-vous d'avoir des politiques de sécurité et des procédures clairement définies pour prévenir de telles attaques.

Question 7: Quels outils de sécurité utilisez-vous ?

Réponse: ['vpn']

Conseil: Vous devriez prioriser pare-feu, antivirus et gestionnaire de mot de passe pour renforcer la sécurité.

Conseils de Cybersécurité

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. Je recommande l'utilisation d'une passphrase, un mot de passe long et complexe, par exemple : "Ch@tN0ir_&_D0gBI@nc!". Risques : accès non autorisés, interceptions de données.

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: Vous pourriez également envisager de restaurer les sauvegardes pour récupérer les données perdues, analyser la faille de sécurité pour la corriger, informer les parties prenantes internes et externes, ainsi que mettre en place des mesures de prévention supplémentaires. Un plan d'urgence en cas de cyberattaque est crucial pour une réponse rapide et efficace, la réduction des dommages et la reprise des activités normales.

Question 10: Quel est votre domaine d?activité ?

Réponse: Boucherie

Conseil: Bien sûr. Voici trois exemples d'attaques qui ont ciblé des entreprises de boucherie :

1. Attaque par ransomware bloquant l'accès aux données clients, demandant une rançon en échange de la clé de déchiffrement.

Conseils de Cybersécurité

2. Vol de données sensibles telles que les coordonnées bancaires des clients à des fins de fraude.

3. Tentative de phishing envoyant des e-mails frauduleux se faisant passer pour des fournisseurs pour obtenir des informations confidentielles.

Résumé global des conseils

Voici un résumé des conseils de sécurité pour Test tb SARL :

Pour sécuriser vos 0-10 ordinateurs et périphériques :

- Mettez à jour régulièrement les systèmes d'exploitation et les logiciels.
- Utilisez des mots de passe robustes et différents pour chaque appareil.
- Installez un antivirus et un pare-feu sur tous les appareils.

Pour sécuriser vos données stockées dans le cloud :

- Utilisez des services cloud réputés et sécurisés.
- Chiffrez vos données avant de les stocker.
- Mettez en place une authentification forte pour limiter l'accès.

Pour sécuriser le partage de données en interne :

- Définissez des règles strictes d'accès aux données.
- Chiffrez les données sensibles lors de leur transmission.

Conseils relatifs aux logiciels utilisés :

- Pour les logiciels de comptabilité : Effectuez des sauvegardes régulières et mettez à jour fréquemment.

Conseils de Cybersécurité

- Pour les logiciels CRM : Limitez l'accès aux informations sensibles et mettez à jour régulièrement.

Concernant la sensibilisation à la cybersécurité :

- Offrez des formations à vos employés chaque année.

- Sensibilisez-les aux risques liés au social engineering sur les réseaux sociaux.

Outils de sécurité recommandés :

- Priorisez pare-feu, antivirus et gestionnaire de mot de passe.

Pour sécuriser votre réseau wifi :

- Utilisez une passphrase complexe pour votre mot de passe wifi.

En cas de cyberattaque :

- Prenez des mesures telles que restauration des sauvegardes, analyse et correction des failles, et communication avec les parties prenantes.

Conseil spécifique pour les boucheries :

- Soyez vigilant contre les attaques de ransomware, le vol de données sensibles et le phishing.

Restez proactif et suivez ces conseils pour renforcer la cybersécurité de votre entreprise de façon efficace.