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: Vous pouvez sécuriser vos dispositifs en :

1. Mettant à jour régulièrement les logiciels.

2. Utilisant des mots de passe forts et les changeant régulièrement.

3. Mettant en place une solution de protection antivirus/antimalware sur chaque appareil.

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

Réponse: cloud

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

2. Chiffrez vos données avant de les stocker dans le cloud pour garantir leur confidentialité.

3. Mettez en place des politiques de gestion des accès pour contrôler qui peut consulter vos données.

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

Réponse: interne

Conseil: Pour sécuriser le partage de données sur un réseau interne, je vous conseille :

Conseils de Cybersécurité

1. Chiffrez les données sensibles avant de les partager pour éviter tout accès non autorisé.

2. Utilisez des protocoles de sécurité comme VPN pour établir des connexions sécurisées entre les utilisateurs.

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

Réponse: ['comptabilité', 'crm', '']

Conseil: Pour la comptabilité : 1. Mettez à jour régulièrement le logiciel pour corriger les failles de sécurité. 2. Limitez l'accès aux informations sensibles uniquement au personnel autorisé.

Pour le CRM : 1. Utilisez des mots de passe forts et changez-les régulièrement pour sécuriser l'accès. 2. Sauvegardez régulièrement vos données pour éviter les pertes en cas d'attaque.

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 essentielle pour sensibiliser vos employés aux risques. Investissez dès maintenant.

Conseil : Planifiez des sessions de sensibilisation annuelles pour maintenir les connaissances à jour.

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

Conseils de Cybersécurité

Réponse: ['twitter', 'instagram', '']

Conseil: Sur Twitter et Instagram, il existe plusieurs risques auxquels vous pourriez être exposé en termes de sécurité. Voici quelques-uns des risques les plus courants :

1. Phishing : Il s'agit d'une technique utilisée par les cybercriminels pour obtenir des informations sensibles telles que des identifiants de connexion, des mots de passe ou des données de carte de crédit en se faisant passer pour une entité de confiance. Par exemple, un message sur Twitter ou Instagram vous invitant à cliquer sur un lien pour prétendument gagner un prix, mais qui en réalité vous redirige vers un site malveillant conçu pour voler vos informations.

2. Hameçonnage (ou "phishing" en anglais) : Cette technique consiste à envoyer des messages frauduleux aux utilisateurs pour les inciter à révéler des informations personnelles. Par exemple, un faux message d'Instagram vous demandant de vérifier vos identifiants en cliquant sur un lien qui vous redirige vers un site de phishing.

3. Ingénierie sociale : Il s'agit d'une méthode utilisée par les cybercriminels pour manipuler les utilisateurs et leur faire divulguer des informations confidentielles. Par exemple, un attaquant pourrait se faire passer pour un employé de votre entreprise sur Twitter et demander des informations sensibles à vos employés.

Il est donc essentiel d'être vigilant et de sensibiliser votre équipe aux risques potentiels liés à l'utilisation des réseaux sociaux. Assurez-vous que vos comptes sont sécurisés avec des mots de passe forts, activez l'authentification à deux facteurs si possible, et formez régulièrement vos employés sur les bonnes pratiques en matière de sécurité en ligne.

Conseils de Cybersécurité

Question 7: Quels outils de sécurité utilisez-vous ?

Réponse: ['vpn']

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

Les outils antivirus et pare-feu sont essentiels pour protéger contre les malwares et les attaques externes. Le gestionnaire de mots de passe permet de renforcer la sécurité des comptes en ligne et de limiter les risques d'attaques par force brute.

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 vous recommande d'utiliser une passphrase composée de plusieurs mots pour renforcer la sécurité, par exemple "ChatsBleusDormir12!". Risques d'un réseau wifi mal sécurisé : accès non autorisé, interception de données, attaques de type "homme du milieu".

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 après une cyberattaque, vous pourriez envisager de mettre en place une procédure de réponse à incident plus détaillée, de réaliser une enquête interne approfondie pour identifier la cause racine de l'attaque, de mettre en place des solutions de protection

supplémentaires et de sensibiliser votre personnel à la sécurité informatique.

Un plan d'urgence en cas de cyberattaque est essentiel pour minimiser les dommages, réagir rapidement et efficacement face à une attaque, limiter la propagation de la menace, protéger les données sensibles, préserver la réputation de l'entreprise et assurer la continuité des activités.

Question 10: Quel est votre domaine d?activité ?

Réponse: Boucherie

Conseil: 1. L'attaque par rançongiciel (ransomware) où des cybercriminels ont chiffré les données de la boucherie, exigeant une rançon pour les déchiffrer.

2. L'attaque de phishing où des employés ont reçu des emails frauduleux demandant des informations sensibles ou des identifiants de connexion.

3. L'attaque de l'homme du milieu (Man-in-the-Middle) où un attaquant a intercepté les communications entre la boucherie et ses fournisseurs, compromettant les transactions.

Résumé global des conseils

Résumé des conseils pour Test tb SARL :

Sécurité des dispositifs :

- Mettre à jour régulièrement les logiciels.
- Utiliser des mots de passe forts et les changer régulièrement.

Conseils de Cybersécurité

- Mettre en place une solution de protection antivirus/antimalware.

Sécurité des données stockées dans le cloud :

- Utiliser une authentification à deux facteurs.
- Chiffrer les données avant de les stocker.
- Mettre en place des politiques de gestion des accès.

Sécurité du partage de données en interne :

- Chiffrer les données sensibles avant de les partager.
- Utiliser des protocoles de sécurité comme VPN.

Sécurité des logiciels de gestion :

- Mettre à jour régulièrement les logiciels.
- Limiter l'accès aux informations sensibles.
- Utiliser des mots de passe forts et sauvegarder régulièrement les données.

Sensibilisation à la cybersécurité :

- Investir dans des formations en cybersécurité.
- Planifier des sessions de sensibilisation annuelles.

Sécurité des réseaux sociaux professionnels :

- Être vigilant face au phishing, hameçonnage et ingénierie sociale.
- Utiliser des mots de passe forts et activer l'authentification à deux facteurs.

Outils de sécurité recommandés :

Conseils de Cybersécurité

- Antivirus, pare-feu et gestionnaire de mot de passe.

Sécurité du réseau wifi :

- Utiliser une passphrase sécurisée plutôt qu'un mot de passe simple (ex. : "ChatsBleusDormir12!").

Gestion après une cyberattaque :

- Mettre en place une procédure de réponse à incident détaillée.

- Réaliser une enquête interne pour identifier la cause racine.

- Sensibiliser le personnel et renforcer les mesures de protection.

Sécurité dans le domaine de la boucherie :

- Identifier les risques comme le rançongiciel, le phishing et l'homme du milieu.

- Mettre en place des mesures de protection adaptées.