Conseils de Cybersécurité

Nom de l'entreprise: Helvetcontrol SA

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

Réponse: 0-10

Conseil: Votre petite entreprise peut améliorer sa cybersécurité en suivant ces conseils :

1. Mettez à jour régulièrement vos logiciels pour corriger les failles de sécurité.

2. Utilisez des mots de passe forts et uniques pour chaque périphérique pour empêcher les intrusions.

3. Installez un antivirus sur tous les appareils pour détecter et bloquer les logiciels malveillants.

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

Réponse: cloud

Conseil: 1. Utilisez l'authentification à deux facteurs pour sécuriser l'accès.

2. Chiffrez vos données avant de les stocker sur le cloud pour renforcer la sécurité.

3. Assurez-vous de choisir un fournisseur de cloud réputé et fiable pour garantir la sécurité.

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

Réponse: mixte

Conseil: 1. Utilisez des protocoles de chiffrement pour protéger les données en transit sur les réseaux internes et externes.

Conseils de Cybersécurité

2. Mettez en place des mesures d'authentification forte pour contrôler l'accès aux données sensibles.

3. Segmentez votre réseau en zones sécurisées pour limiter la propagation en cas d'incident de sécurité.

4. Mettez en place des politiques de gestion des accès et des autorisations pour restreindre les droits d'accès.

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

Réponse: ['Infradata']

Conseil: Pour maintenir le logiciel ['Infradata'] sécurisé :

1. Assurez-vous de mettre à jour régulièrement le logiciel pour bénéficier des correctifs.

2. Limitez l'accès aux informations sensibles en configurant correctement les autorisations d'accès.

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: Il est crucial de former vos employés en cybersécurité pour protéger vos données. Conseil : Formez-les annuellement.

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

Réponse: ['linkedin', 'facebook', 'instagram', '']

Conseils de Cybersécurité

Conseil: Sur les réseaux sociaux tels que LinkedIn, Facebook et Instagram, il y a plusieurs risques potentiels en matière de sécurité.

1. LinkedIn : Sur LinkedIn, les risques principaux sont liés à la divulgation d'informations professionnelles sensibles telles que votre poste, votre entreprise ou vos relations professionnelles. Les attaquants peuvent utiliser ces informations pour mener des attaques de phishing ciblées ou des tentatives d'ingénierie sociale.

Exemple de social engineering sur LinkedIn : Un attaquant peut créer un faux profil LinkedIn prétendant être un recruteur. Il peut ensuite contacter des employés de votre entreprise en se faisant passer pour un recruteur qui propose de meilleures offres d'emploi. Les employés peuvent être incités à divulguer des informations confidentielles sans même s'en rendre compte.

2. Facebook : Sur Facebook, les risques incluent la divulgation d'informations personnelles, les attaques de phishing à travers des faux concours ou des messages malveillants, ainsi que la propagation de fausses informations.

3. Instagram : Sur Instagram, les risques sont similaires à ceux de Facebook, avec une attention particulière à la divulgation d'informations personnelles à travers des photos, des lieux visités ou des interactions avec d'autres utilisateurs.

Il est important de sensibiliser les employés à rester vigilants et à ne pas divulguer d'informations sensibles sur les réseaux sociaux. Soyez prudent quant aux demandes de connexion ou aux messages provenant de personnes inconnues, même si elles prétendent être des recruteurs ou des collègues. Vous devez également vous assurer que vos paramètres de confidentialité sont

correctement configurés pour limiter l'accès à vos informations.

Question 7: Quels outils de sécurité utilisez-vous ?

Réponse: ['antivirus', 'firewall', 'vpn', 'sauvegarde']

Conseil: Vous devriez considérer en priorité un gestionnaire de mots de passe pour renforcer la sécurité.

Les gestionnaires de mots de passe sont essentiels pour sécuriser les identifiants et les mots de passe utilisés par les employés. Cela permet de garantir des mots de passe forts, uniques et de limiter les risques liés à la réutilisation des mots de passe.

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

Réponse: un mot de passe élevé (Mg7@Lkf232-!)

Conseil: Le mot de passe que vous utilisez semble être sécurisé. Cependant, une passphrase pourrait être préférable car plus facile à retenir pour les utilisateurs tout en maintenant un niveau élevé de sécurité.

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: ['vérification des logs', ' contact préstataire informatique', ' isoler les sauvegarde', ' conservation des preuves via screenshot']

Conseils de Cybersécurité

Conseil: Pour être plus efficace lors d'une cyberattaque, vous pourriez ajouter les actions suivantes : impliquer une équipe de réponse à incident, mettre en place une communication claire aux parties prenantes, renforcer la supervision du réseau pour détecter d'autres intrusions et évaluer régulièrement vos mesures de sécurité pour les améliorer.

Un plan d'urgence en cas de cyberattaque est crucial car il permet de réagir rapidement et efficacement face à une intrusion. Il aide à limiter les dégâts, à protéger les données sensibles, à minimiser les temps d'arrêt et à rétablir les services le plus rapidement possible.

Question 10: Quel est votre domaine d?activité ?

Réponse: Contrôle installation électrique

Conseil: 1. Des attaques de phishing ciblant les employés de PME du secteur électrique pour obtenir des informations sensibles.

2. Des ransomwares bloquant l'accès aux systèmes de contrôle des installations électriques, paralysant ainsi l'activité de l'entreprise.

3. Des attaques par force brute visant les connexions à distance aux systèmes de contrôle, compromettant la sécurité des installations.

Résumé global des conseils

Conseils pour Helvetcontrol SA:

Cybersécurité pour une petite entreprise (0-10 ordinateurs et périphériques):

- Mettre à jour régulièrement les logiciels

Conseils de Cybersécurité

- Utiliser des mots de passe forts et uniques

- Installer un antivirus sur tous les appareils.

Stockage des données dans le cloud:

- Utiliser l'authentification à deux facteurs

- Chiffrer les données avant de les stocker

- Choisir un fournisseur de cloud réputé et fiable.

Partage des données mixte au sein de l'entreprise:

- Utiliser des protocoles de chiffrement

- Mettre en place des mesures d'authentification forte

- Segmenter le réseau en zones sécurisées

- Mettre en place des politiques de gestion des accès.

Gestion du logiciel Infradata:

- Mettre à jour le logiciel régulièrement

- Limiter l'accès aux informations sensibles.

Formation en cybersécurité pour les employés:

- Former les employés annuellement.

Réseaux sociaux professionnels utilisés:

- Sensibiliser sur les risques potentiels

- Configurer les paramètres de confidentialité.

Conseils de Cybersécurité

Outils de sécurité utilisés:

- Considérer l'utilisation d'un gestionnaire de mots de passe.

Sécurité du réseau wifi:

- Envisager l'utilisation d'une passphrase.

Actions post-cyberattaque:

- Impliquer une équipe de réponse à incident
- Communiquer clairement aux parties prenantes
- Renforcer la supervision du réseau.

Domaine d'activité (Contrôle installation électrique):

- Se méfier des attaques de phishing ciblant les employés
- Se prémunir contre les ransomwares
- Renforcer la sécurité des connexions à distance.