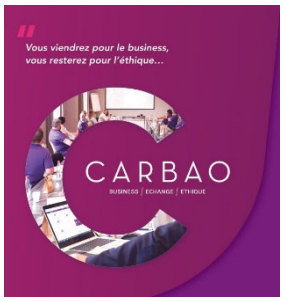

COMPTE RENDU REUNION CARBAO CYBERSECURITE

La discussion s'est concentrée sur plusieurs aspects cruciaux :

1. **Protection antivirus (ESET ADVANCED PROTECT)**: Importance de se prémunir contre les virus et logiciels espions (spywares).
2. **Sécurité des prélèvements bancaires** : Dangers de la diffusion de son IBAN sur sa facture ou son site WEB, des prélèvements non autorisés sont possibles, exposant à des risques de prélèvements non autorisés. Vérification systématique des IBAN pour éviter les fraudes.
3. **Gestion des mots de passe** : Adoption de mots de passe sécurisés et utilisation d'outils comme **LastPass** pour leur gestion.
4. **Sécurité des Boites mails et gestion des spams : Utilisation** de mot de passe différents pour les boites et utilisations d'outils type **MailInBlack**
5. **Protection des données clients** : Mise en œuvre de bonnes pratiques pour éviter les piratages et garantir leur confidentialité. Sauvegardes interne, externe (cloud) manuel ou automatisées.

1- Protection antivirus

Un antivirus efficace est essentiel pour protéger les systèmes contre les virus, les spywares et autres malwares. Ces menaces peuvent compromettre les données personnelles et professionnelles, ralentir les ordinateurs, ou pire, permettre des accès non autorisés. Il est recommandé de choisir un antivirus réputé, de le maintenir à jour, et de réaliser des analyses régulières.

Frédéric LOPES vous conseil ESET ADVANCED PROTECTED*, il vous propose une offre très intéressante sur l'abonnement à cet antivirus Professionnel 30€/PC/an au lieu de 47€/PC/an (pour plus d'information n'hésitez pas à le contacter)

2- Sécurité Bancaires et prévention des fraudes (quelques solutions)

Vérification régulière des comptes bancaires

- Banques en ligne sécurisées : La plupart des banques offrent des interfaces en ligne avec des outils d'alertes automatiques pour signaler des mouvements suspects ou inhabituels. Par exemple :
    - Crédit Agricole Espace Pro propose des notifications pour chaque transaction.
    - Banque Populaire Cyberplus offre des options de paramétrage d'alertes.

Gestion des mandats SEPA

- Sepa Manager : Une solution dédiée à la gestion des mandats SEPA, permettant de vérifier et valider chaque prélèvement. Il s'assure que seuls les prélèvements autorisés sont traités.
- GoCardless : Un outil qui facilite les paiements récurrents tout en assurant un contrôle total sur les autorisations de prélèvement.
-

Automatisation des contrôles avec des logiciels

- Sage Business Cloud : En plus de gérer la comptabilité, ce logiciel inclut des fonctionnalités de vérification des paiements et des prélèvements.
- Esker : Ce logiciel optimise la gestion des factures et prélèvements, offrant un suivi détaillé des transactions.
-

Renforcement de la sécurité avec des dispositifs

- Token et authentification forte : De nombreuses banques proposent des dispositifs physiques ou des applications mobiles pour valider chaque transaction (ex. : Secur'Pass de Crédit Agricole ou Digipass).
- Vérification des prélèvements par signature électronique : Avec des outils comme DocuSign, vous pouvez ajouter une étape de validation sécurisée pour autoriser les prélèvements sensibles.

Utilisation d'agrégateurs bancaires

- Bankin' ou Linxo : Ces applications permettent de centraliser toutes les transactions de plusieurs comptes bancaires et d'analyser les prélèvements suspects ou non autorisés.
  Ces solutions, associées à une vigilance régulière et une sensibilisation des équipes, permettent de limiter les risques liés aux prélèvements non autorisés tout en renforçant la sécurité financière.

3- Gestion des mots de passe : bonnes pratiques et sécurité dans les navigateurs

- Les mots de passe doivent être longs, uniques et complexes. Les gestionnaires intégrés aux navigateurs (comme Chrome ou Firefox) offrent une solution pratique avec synchronisation entre appareils, mais ils présentent des risques si le compte principal est compromis.

Conseils pour sécuriser les mots de passe dans un navigateur :

- Active l'authentification à deux facteurs (2FA) sur le compte synchronisé.
- Utilise un mot de passe principal (disponible sur Firefox).
- Évite d'enregistrer les mots de passe des comptes critiques (banques, santé).
- Assure-toi que le navigateur est à jour.
- Pour une sécurité renforcée, privilégie des gestionnaires dédiés comme LastPass, Dashlane ou 1Password, qui offrent un chiffrement avancé et des outils d'audit. Une combinaison des deux solutions peut être idéale selon les besoins.

4. Sécurité des mails et gestion des spams

Les emails restent une porte d'entrée majeure pour les cyberattaques, notamment via les spams, le phishing ou les pièces jointes malveillantes. Une bonne gestion et des outils adaptés permettent de réduire ces risques.

Bonnes pratiques pour sécuriser les mails :

- Activer l'authentification à deux facteurs (2FA) sur les comptes mail pour empêcher tout accès non autorisé.
- Utiliser des mots de passe forts et uniques pour chaque compte mail.
- Vérifier les expéditeurs et les liens avant de cliquer ou de télécharger des pièces jointes.
- Ne jamais répondre aux spams pour éviter de confirmer que l'adresse est active.

Outils pour gérer les spams efficacement :

- Filtres anti-spam intégrés : Les services comme Gmail, Outlook ou ProtonMail intègrent des solutions puissantes pour détecter et isoler automatiquement les spams.
- Solutions professionnelles : Des outils comme MailinBlack* SpamTitan ou MailCleaner offrent des protections avancées contre les spams, le phishing et les malwares, idéales pour les entreprises.
- Surveillance des domaines : Les entreprises peuvent utiliser des protocoles comme SPF, DKIM et DMARC pour éviter que leurs domaines soient usurpés.

5. Protection des données clients : Stratégies de sécurité et sauvegardes efficaces

La protection des données clients est essentielle pour préserver leur confidentialité et éviter les piratages. Il est crucial d'adopter des bonnes pratiques de sécurité, telles que le chiffrement des données sensibles et l'accès restreint aux informations.

Les sauvegardes régulières sont une mesure clé pour garantir la récupération des données en cas de sinistre. Elles peuvent être réalisées de manière interne sur des serveurs sécurisés ou via des solutions externes, telles que le cloud. **Les sauvegardes cloud offrent une redondance et une accessibilité renforcées**, ce qui permet de protéger les données contre des pannes locales ou des attaques physiques.

Les disques durs externes et **les NAS (Network Attached Storage)** offrent une alternative locale, permettant de conserver une copie des données en toute sécurité. Un NAS est particulièrement utile pour les entreprises, car il permet un stockage centralisé avec des options de redondance (RAID) pour éviter la perte de données en cas de défaillance du disque.

Les sauvegardes peuvent être manuelles ou automatisées, selon les besoins de l'entreprise. Les sauvegardes automatisées sont recommandées pour garantir une fréquence régulière sans risque d'oubli. De plus, il est essentiel de tester régulièrement les sauvegardes pour s'assurer qu'elles sont fonctionnelles et récupérables en cas de besoin.

Une stratégie combinant stockage local (disques durs, NAS) et cloud, avec des mesures de sécurité appropriées comme le chiffrement et l'authentification multi-facteurs, garantit une protection optimale des données clients.

*Précision sur ESET Advanced Protect (offre AFTECH informatique Partenaire)

Un antivirus performant est crucial pour protéger les systèmes contre les menaces numériques. ESET Advanced Protect se distingue par ses fonctionnalités avancées qui garantissent une sécurité renforcée :

- **Protection multicouche** : Analyse proactive des menaces, y compris les ransomwares, les malwares et les logiciels espions, avant qu'ils ne puissent causer des dommages.
- **Détection basée sur l'intelligence artificielle** : ESET utilise des algorithmes avancés pour détecter et bloquer les nouvelles menaces, même inconnues, en s'appuyant sur le machine learning.
- **Protection en temps réel** : Surveillance continue des activités réseau et des fichiers pour bloquer immédiatement toute intrusion suspecte.
- **Faible impact sur les performances** : Optimisé pour fonctionner discrètement en arrière-plan sans ralentir les systèmes, idéal pour les environnements professionnels.
- **Gestion centralisée** : Parfait pour les entreprises, ESET permet de superviser et de gérer à distance la sécurité de plusieurs appareils à partir d'une console unique.
- En adoptant une solution comme ESET Advanced Protect, les entreprises et particuliers peuvent bénéficier d'une protection complète et fiable tout en maintenant leur productivité.

*focus sur Mailinblack (offre AFTECH informatique Partenaire)

Les emails sont une cible privilégiée pour les cyberattaques, notamment via les spams et les tentatives de phishing. Des solutions comme **Mailinblack** permettent de renforcer la sécurité et de limiter les risques liés aux courriels malveillants.

Mailinblack : une solution clé en main

Mailinblack se distingue par son approche proactive et conviviale :

- **Filtrage intelligent** : Grâce à une analyse avancée, Mailinblack bloque les spams, les mails frauduleux et les tentatives de phishing avant qu'ils n'atteignent la boîte de réception.
- **Challenge humain** : Les expéditeurs inconnus doivent valider leur identité via une procédure simple, éliminant automatiquement les robots et les sources suspectes.
- **Personnalisation** : Les utilisateurs peuvent ajuster les paramètres pour créer des listes blanches (expéditeurs approuvés) et noires (expéditeurs bloqués).
- **Protection des données** : Mailinblack est conforme au RGPD et garantit une confidentialité maximale pour les entreprises et les particuliers.

Pourquoi choisir une solution comme Mailinblack ?

- Réduction drastique des spams et des risques d'intrusion.
- Gain de temps grâce à une boîte mail mieux triée.
- Sécurité accrue pour les entreprises manipulant des données sensibles.

En adoptant une solution comme Mailinblack, on assure une protection proactive contre les menaces liées aux emails, tout en améliorant la productivité.

Pour plus d'infos sur les logiciels ou des renseignements sur tous sujets de cybersécurité et Informatique divers n'hésitez pas à me contacter. Un Audit gratuit de votre parc offert par AFTECH INFORMATIQUE.

LOPES Frédéric 06 13 66 70 19