CAFÉ des bonnes pratiques

Sécurité informatique

COMMENT PROTÉGER MON ENTREPRISE ET RESPECTER LES DROITS DE MES CLIENT·E·S ?

A MISE EN SITUATION

1 SITUATION INITIALE

Une entreprise de e-commerce genevoise propose des paniers de produits régionaux à composer soi-même en ligne, selon l'offre saisonnière des producteur·trice·s. Elle a créé une plateforme informatique pour permettre à ses fournisseur·sseuse·s et producteur·trice·s de gérer eux·elles-mêmes leurs produits et aux client·e·s de les visualiser selon l'arrivage de saison. En outre, la plateforme effectue les tâches administratives et comptables et les factures client·e·s. Une formule à succès qui propose une activité de vente en lien avec le développement durable puisqu'elle favorise les circuits courts et la proximité tout en tirant les bénéfices de la transition numérique, dite de « plateformisation », de manière équitable.

2 DÉCLENCHEUR

Jean-Baptiste, chargé de la comptabilité de l'entreprise, consulte journalièrement le système d'information ainsi que l'état des comptes sur le site Internet de la banque de l'entreprise. Il pratique le télétravail depuis son domicile quelques jours par mois. Pour jongler facilement entre les différents comptes, y compris ses comptes de messagerie personnels, il a choisi un mot de passe unique et facile à mémoriser - 060811 - soit les années de naissance de ses trois enfants.

3 PÉRIPÉTIES

Le mot de passe a été très facilement reconstitué par un pirate malveillant grâce à un simple logiciel disponible sur internet lorsque Jean-Baptiste travaillait à son domicile où les connexions sans fils avec son ordinateur portable professionnel n'étaient pas suffisamment protégées. L'entreprise se fait voler ses adresses client·e·s et fournisseur·sseuse·s. Les client·e·s, choqué·e·s et mécontent·e·s, entament une procédure judiciaire collective contre l'entreprise qu'ils tiennent pour responsable de la fuite de données.

4 RÉSOLUTION

L'entreprise fait appel à des spécialistes qui réalisent un diagnostic de sa sécurité informatique. Elle décide également d'investir pour sécuriser son système et se dote d'une assurance pour les risques non couverts. De plus, elle impose un règlement strict à ses employé·e·s afin qu'il·elle·s dissocient vie numérique privée et professionnelle. L'action en justice échoue, car l'entreprise n'ayant que des fournisseur·sseuse·s et des client·e·s basés en Suisse, elle n'est pas concernée par le Règlement européen général sur la protection des données (RGPD) et la loi suisse sur la protection des données n'est pas encore en vigueur.

5 SITUATION FINALE

Malgré une image ternie auprès de ses client·e·s, l'entreprise a fait parler d'elle dans la presse avec cette mésaventure et voit les nouveaux client·e·s affluer. Comme son environnement numérique est désormais ultra sécurisé et adapté au RGPD, l'entreprise envisage désormais d'étendre ses services aux producteur·trice·s et consommateur·trice·s transfrontalier·e·s du Grand Genève, tout en gardant son concept de proximité.

Chambre de l'économie sociale et solidaire APRÈS-GE

www.apres-ge.ch

LOTERIE ROMANDE

AVEC LE SOUTIEN DE LA VILLE DE GENÈVE

B BONNES PRATIQUES CONCRÈTES

Comprendre la vulnérabilité informatique

- **Que faut-il protéger ?** La confidentialité, l'intégrité, la disponibilité et la traçabilité des données sont à préserver absolument, pour des raisons de sécurité, mais aussi légales (Règlement européen général sur la protection des données : RGPD).
- **Que recherchent les pirates malveillant•e•s ?** Toute entité est une cible intéressante pour les personnes mal intentionnées. C'est pourquoi il est crucial de rester vigilant. Les demandes de rançon pour récupérer des données, les piratages à but d'espionnage ou les vols d'identités bancaires sont des pratiques courantes qui pour la plupart contribuent à financer le crime organisé.
- **Quelles conséquences ?** La perte d'argent, la mauvaise réputation vis-à-vis de ses clients et des poursuites pénales sont à craindre en cas de piratage.

L'anticipation est la meilleure protection

- **Évaluer les risques.** Réaliser un audit de sécurité afin d'évaluer le risque encouru en cas d'attaques, de le chiffrer et d'estimer les investissements à mettre en œuvre pour les éviter ou les anticiper. Les risques peuvent être couverts par des assurances et des entreprises spécialisées proposent des services, comme le « Disaster recovery plan » d'Itopie.
- **Connaître la loi.** L'Europe applique son Règlement général sur la protection des données (RGPD) depuis mai 2018, tandis que la révision de la loi suisse aboutira en 2019. Les entreprises suisses ayant des clients en Europe sont déjà concernées. Elles doivent récolter un minimum de données, demander clairement le droit d'utiliser une adresse e-mail et respecter la majorité numérique. Un•e internaute peut exiger l'effacement de ses données, transférer toutes ses données personnelles d'un prestataire à l'autre et désormais intenter des actions juridiques collectives contre une société.

Adopter les bons comportements au quotidien

- **xBM46&38mDp@supermotdepasse.** Choisir un mot de passe de douze caractères au minimum, comprenant des minuscules, des majuscules, des chiffres, des lettres et des caractères spéciaux. Le mot de passe doit être unique pour chaque service. Se faire aider par des logiciels de gestion de mots de passe (comme KeepassXC en libre) et/ou des moyens mnémotechniques pour s'en souvenir. Un mot de passe long et complexe n'a pas besoin d'être changé fréquemment.
- **Sans fil, mais pas sans filet.** Le sans-fil étant accessible à tou•te•s dans un périmètre donné, il faut sécuriser les accès Wi-Fi. Un ou plusieurs pare-feux sont nécessaires pour stopper les connexions ou les autoriser, permettant de filtrer de manière fine les informations. Éviter les accès gratuits non protégés lors des déplacements.

- **Les deux facettes des mises à jour.** Toutes les mises à jour («update»: ex. passage d'une version 3.2 à 3.3) sont à effectuer immédiatement, surtout si elles concernent des failles de sécurité. Les améliorations de système ou de logiciels («upgrade»: ex. passage d'une version 4 à 5) peuvent au contraire apporter des régressions, il est donc préférable d'attendre quelque temps en évitant toutefois de prendre trop de retard pour ne pas se rendre vulnérable.
- **Sauvegarder régulièrement.** Veiller à ses propres données en effectuant des sauvegardes quotidiennes ou hebdomadaires permet de récupérer ses données en cas de panne ou de cyberattaque.
- **Toutes les technologies intelligentes sont des ordinateurs.** S'assurer que tous les dispositifs connectés sont protégés (tablettes, smartphones, caméras vidéo, détecteurs à incendie, bracelets ou autres objets connectés, etc.).
- **Achats en ligne de mire.** Avant d'effectuer un paiement, contrôler la présence d'un cadenas dans la barre d'adresse ou dans le navigateur, vérifier que «https://» apparaît dans l'adresse du site Internet et l'exactitude de cette adresse. La méthode d'authentification en deux étapes (mot de passe puis code dynamiquement généré) est la plus fiable. Le code de confirmation peut être envoyé via SMS. Il existe également des applications OTP (One Time Password) ou des clefs USB cryptographiques de sécurité, telles que Yubikey ou Nitrokey (www.nitrokey.com).
- **La messagerie, une porte d'entrée facile.** Prendre des précautions surtout dans le traitement des liens URL et des pièces jointes. Ne pas ouvrir les pièces jointes provenant d'expéditeur•trice•s inconnu•e•s et désactiver leur ouverture automatique. Vérifier la cohérence des liens transmis avant de cliquer dessus: ils doivent contenir le nom de domaine officiel, le tout préfixé par https://. Le «s» assure le chiffrement de la communication entre le navigateur et le serveur. Ne jamais fournir d'informations personnelles ou confidentielles et n'utiliser que des adresses électroniques dédiées.
- **Gestion de confiance.** Bien connaître ses utilisateur•trice•s et ses fournisseur•sseuse•s, consulter les revues de fiabilité online. et, si possible, s'entourer de prestataires locaux. Télécharger les programmes depuis les sites officiels des éditeur•trice•s.
- **Dissociation professionnelle et privée.** Séparer les usages personnels des usages professionnels, surtout au niveau des messages électroniques et du stockage de données.
- **Préserver son identité numérique.** Divulguer des informations personnelles ou professionnelles avec une extrême prudence, surtout sur les réseaux sociaux. Refuser systématiquement le partage de données. Vérifier les paramètres de sécurité et de confidentialité.

DOCUMENTS RESSOURCE

- *Guide de survie d'Itopie*
- *Sécurité de l'information: aide-mémoire*
- *Guide des bonnes pratiques du CPME*
- *Capsule vidéo «Sécurité informatique»*

SUR NOTRE SITE

www.apres-ge.ch

EXPERTISE INVITÉE

Itopie Informatique
Kyos