B • CONTACT GROUP

PROVENCE • AZUR • ALPES
www.bcontact.fr

Votre prestataire vous rappelle les bonnes pratiques pour sécuriser vos systèmes d'information

Alors que le numérique fait désormais partie intégrante de nos vies personnelles et professionnelles, le niveau de sécurité appliqué dans la plupart des entreprises est très largement lacunaire. Les nouvelles technologies, porteuses de nouveaux risques pesant lourdement sur les entreprises, imposent de prendre en compte la sécurité dans nos usages.

L'acquisition de réflexes simples et de bon sens permet de sécuriser votre usage de l'informatique. Soucieux de votre sécurité, votre prestataire vous conseille et vous informe sur les risques et les moyens de vous en prémunir en acquérant des réflexes simples.

Votre prestataire, dans le cadre de son obligation de conseil et d'information, vous invite à adopter les bonnes pratiques et à mettre en œuvre sans délai l'ensemble des recommandations ci-dessous.

Préservez vos données

Nul ne pouvant garantir zéro défaillance ou zéro intrusion, les sauvegardes sont indispensables et doivent être réalisées à des échéances calculées en fonction de la quantité de données qui peut être perdue par l'entreprise sans mettre son exploitation en danger. Les sauvegardes, quel que soit le support, ne doivent pas être conservées sur le même lieux que les données.

Attention, selon l'usage, la surveillance de la bonne exécution des sauvegardes est de votre ressort. N'hésitez pas à solliciter votre prestataire pour la mise en place d'un contrat de supervision si vous souhaitez externaliser cette fonction vitale.

Une sauvegarde fiable est une sauvegarde testée. Il est nécessaire de planifier des tests réguliers. En outre, Cloud ne signifie pas sauvegarde. Vos données dans le Cloud ne sont pas implicitement sauvegardées.

Faites les mises à jour

Les mises à jour de vos systèmes d'exploitation, logiciels et applications doivent être réalisées, idéalement automatiquement, sinon, téléchargez les correctifs de sécurité disponibles.

Un antivirus de dernière génération, piloté et centralisé est indispensable sur tous vos postes et vos serveurs de fichiers. En cas d'alerte, il faut prévenir votre prestataire. Ne négligez pas non plus les appareils mobiles, soyez aussi prudents avec les smartphones et tablettes qu'avec les ordinateurs.

Choisissez vos mots de passe avec soin

Vous devez mettre en place une politique de gestion des mots de passe stricte et réfléchie. Pour vous aider, rendez-vous sur le site www.cybermalveillance.gouv.fr/tous-nos-contenus/

Sécurisez votre accès internet

Votre accès internet doit être protégé par un vrai UTM (United Threat Management). Les services inclus dans les boxes des opérateurs n'offrent AUCUNE sécurité. Par ailleurs, les accès à distance mis à disposition de vos collaborateurs nomades doivent être sécurisés via un accès SSL.

Soyez prudent lors de l'utilisation de la messagerie

Les courriels et pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques. Evitez de cliquer sur les pièces jointes, liens ou messages inconnus.

Sensibilisez vos collaborateurs

Les courriels et pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques. Evitez de cliquer sur les pièces jointes, liens ou messages inconnus.

Sensibilisez vos collaborateurs

Faites de la sécurité un enjeu partagé par l'ensemble des collaborateurs en mettant en place une campagne régulière d'information et de sensibilisation.

Une charte d'utilisation des systèmes d'information qui précisera de manière explicite les droits et devoirs des collaborateurs est indispensable. A défaut, il sera illégal et de votre stricte responsabilité de mener des opérations sur vos systèmes informatiques telles que la récupération d'e-mail après le départ d'un salarié, l'enregistrement des logs en cas de plainte, procédures disciplinaires...

Votre prestataire est là pour vous assister dans toutes ces démarches, et a une obligation de conseil, matérialisée par cette fiche, mais le choix de faire ou de ne pas faire n'appartient qu'à vous !

270, Impasse des Sauvegards
38490 Aoste

Administratif
04 65 13 55 72 • admin@bcontact.fr

Technique
04 92 64 15 84 • b.contact@bcontact.fr

SAS au capital de 450 000 euros • R.C.S. Gap 444 864 383
APE 7022Z • N° TVA INTRACOMMUNAUTAIRE : FR 37 444 864 383 • N° SIRET : 444 864 383 000 39

OCTOBRE - DÉCEMBRE 2019 | N°3

CYBERSECURE

FEDERATION EBEN
ENTREPRISES DU BUREAU ET DU NUMERIQUE

AU SOMMAIRE

A la Une : attaques par mail

QUAND LE GROS POISSON C'EST VOUS !

Les arnaques via messagerie électronique se multiplient et les techniques sont variées. Le mail est la porte d'entrée sur les données personnelles les plus essentielles : lien avec les organismes administratifs (banque, impôt...), comptes des sites d'achat et donc données bancaires... Qui ne consulte pas sa boîte mail plusieurs fois par jour ? De chez soi ou au travail ? De son smartphone ou de son poste informatique ? Les occasions ne manquent pas aux hackers et autres individus malintentionnés pour dérober les données personnelles ou professionnelles d'un utilisateur.

Les techniques les plus diverses

Ainsi, en juin dernier, 2000 comptes en ligne du site Impots.gouv.fr ont été piratés. Les hackers ont ainsi accédé aux données des contribuables concernés et ont modifié leurs déclarations. Bercy s'en est aperçu lorsqu'une avalanche de demandes de renouvellement de mots de passe a déferlé sur le site. En cause, les boîtes mail des contribuables qui n'étaient pas suffisamment protégées et qui ont permis aux pirates d'envoyer des demandes de renouvellement de mots de passe. Depuis, les services fiscaux ont renforcé leur politique de sécurité et se sont empressés d'avertir les contribuables en leur recommandant de mieux sécuriser leurs mots de passe.
Autre cas, autres méthode, celle de l'hameçonnage (ou phishing en anglais) qui consiste à se faire passer pour un tiers de confiance afin de récupérer les données de l'utilisateur. Ainsi, pendant plusieurs mois, 850 000 ordinateurs à travers le monde ont été infectés par le virus « Retadup », chez des particuliers comme dans des entreprises, via des liens frauduleux contenus dans des mails proposant de gagner de l'argent ou encore d'accéder à des photos érotiques. Un clic a donc suffi ! Depuis un serveur basé en Ile-de-France, les pirates ont pu dérober des données de patients et fabriquer de la cryptomonnaie. En tout 140 pays ont été touchés, dont la France. Le réseau criminel à l'origine de ce virus a pu officier pendant plusieurs mois sans que les utilisateurs des ordinateurs infectés ne s'en rendent compte.
De même, un hôpital privé de Nantes a été victime, en mai et juin dernier, de campagnes de mail frauduleux : les salariés de l'établissement ont reçu une invitation à renouveler leurs mots de passe et identifiants de connexion au système informatique de l'établissement. Se faisant, les utilisateurs ont transmis leurs données d'accès qui ont permis aux pirates de pénétrer le système.

Messagerie électronique

LES RÈGLES DE PRUDENCE

- Utilisez des mots de passe différents et complexes pour chaque site et application, à commencer par votre messagerie.
- Ne communiquez jamais d'informations sensibles par messagerie ou téléphone : aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.
- Ne mélangez pas votre messagerie professionnelle et personnelle afin d'éviter les erreurs de destinataire ou de mettre en danger votre entreprise en cas de piratage de votre boîte personnelle (souvent moins bien sécurisée).
- Evitez les réseaux wi-fi publics ou inconnus lorsque vous consultez votre messagerie.
- Ne cliquez pas trop vite sur un lien contenu dans un mail : positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question sans passer par ce lien.
- Vérifiez l'adresse de l'expéditeur avant toute ouverture de mail. Bien souvent, l'origine frauduleuse se détecte à la lecture de l'adresse. Si le doute persiste n'hésitez pas à contacter directement l'organisme concerné pour demander une confirmation.
- Ne relayez pas les canulars et autres chaînes de lettres, porte-bonheur... vous prenez le risque d'accroître la viralité d'un mail frauduleux et de surchargez les systèmes.

Gestion des mots de passe

10 CONSEILS POUR ÊTRE EFFICACE

- Utilisez un mot de passe différent pour chaque service
- Utilisez un mot de passe suffisamment long et complexe
- Utilisez un mot de passe impossible à deviner
- Utilisez un gestionnaire de mot de passe
- Changez votre mot de passe au moindre soupçon
- Ne communiquez jamais votre mot de passe à un tiers
- N'utilisez pas vos mots de passe sur un ordinateur partagé
- Activez la «double authentification» lorsque c'est possible
- Changez les mots de passe par défaut des différents services auxquels vous accédez
- Choisissez un mot de passe particulièrement robuste pour votre messagerie

Petite astuce pour un mot de passe solide et mémorisable

Faites une phrase dont vous vous souviendrez facilement, par exemple «J'aime les gateaux au chocolat de ma grand-mère». Prenez la qsf njðsf mfuusf ef dibrvf npu. fo wfjmmbou è n fuusf dfsubjoft fo nbkvtdvmft fu è usbotgpsn fs dfsubjot nput fo dijdbsft⇩

Cela donne : **J'**alg**O**c**2**mg-m

Cette lettre d'information vous est offerte par votre prestataire

Collez votre logo ici.

Fédération EBEN
69, rue Ampère
75017 Paris
www.federation-eben.com

MEMBRE DU DISPOSITIF
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Directeur de la publication : Loïc Mignotte
Rédaction : Fédération EBEN, Cybermalveillance.gouv.fr
Photos : Unsplash, Adobe Stock
Maquette : Emmanuelle Bauvais