Performance Bretagne

Ressources humaines

41

QUESTIONS RESSOURCES HUMAINES

COMMENT SÉCURISER LES USAGES NUMÉRIQUES DANS MON ENTREPRISE ?

LES PROBLÉMATIQUES DU DIRIGEANT

Vous craignez les risques liés au numérique dans votre entreprise ? Vous voulez fixer des règles pour leur usage par vos collaborateurs ? Renforcer la sécurité des systèmes d'information ?

SÉCURISER LES USAGES NUMÉRIQUES, UNE NECESSITE POUR MON ENTREPRISE

1 | ETRE ACTEUR DE SA SÉCURITÉ

Le numérique prend une part de plus en plus importante dans nos activités professionnelles. Même si votre entreprise est de taille modeste, il est primordial de ne pas négliger sa sécurité et de vous prémunir contre les actes de malveillance informatique dont les risques pourraient peser lourdement sur votre organisation et sa performance.

2 | SENSIBILISER VOS COLLABORATEURS

Pour limiter une grande partie des risques d'incidents liés à la sécurité informatique, la sensibilisation de vos collaborateurs est primordiale. Vous pouvez imposer quelques mesures simples en choisissant avec soin vos mots de passe, en mettant à jour régulièrement vos logiciels, ou encore en protégeant vos données lors des déplacements. Responsabilisez également vos salariés en les sensibilisant ou en les formant à la sécurité informatique.

3 | ETABLIR DES RÈGLES

Mélanger les usages personnels et professionnels augmente les risques d'intrusion ou de vol de vos données. Il est donc recommandé de ne pas faire suivre des messages électroniques professionnels vers des services de messagerie personnelle et de ne pas héberger des données professionnelles sur des équipements ou des stockages personnels et vice-versa.

TÉMOIGNAGES

Protéger mon entreprise

« J'étais loin d'imaginer que le mot de passe que j'avais choisi pour accéder à nos comptes bancaires était une faille dans mon système . Il était peut-être simple à retenir, mais aussi facile à pirater. Maintenant j'utilise un mot de passe alphanumérique que je renouvelle régulièrement. »

Prévenir et se prémunir des attaques

« Récemment, j'ai été sensibilisé au phénomène du "rançongiciels". Vos données sont cryptées par des hackers et ne peuvent être récupérées qu'en échange d'une rançon. C'est vrai que les réseaux de «botnets» recherchent des serveurs mal sécurisés pour y installer des codes malintentionnés. »

Rédiger une charte informatique

« En groupe de travail, nous avons mené une réflexion sur la mise en place d'une charte informatique pour ma entreprise. Elle définit les responsabilités de chacun, les procédures à mettre en place et quelques règles de bon sens. J'ai nommé également un salarié-référent et je le forme régulièrement aux enjeux de la sécurité dans une entreprise. »

DES MOYENS SIMPLES POUR SÉCURISER VOS USAGES NUMÉRIQUES

1 | DRESSER UN ÉTAT DES LIEUX

La première étape consiste à faire un état des lieux et repérer les informations stratégiques de votre entreprise ainsi que les risques associés. Faites l'inventaire de toutes vos informations sensibles ou confidentielles : brevets, fichiers clients, prospects, études de concurrence, orientations stratégiques, contrats, paie, données comptables... Puis recensez les ressources de votre systèmes d'information : ordinateurs, téléphones fixes et portables, accès à internet, messagerie électronique, clés USB, réseau Wi-Fi, Bluetooth… Vous aurez ainsi une vision d'ensemble de vos outils d'information. Cela vous permettra d'évaluer les risques potentiels de votre entreprise et servira de point de départ aux actions à entreprendre.

2 | ADOPTER DES BONNES PRATIQUES

Adoptez au quotidien, des règles simples : distinguez les profils utilisateurs et les droits d'accès associés, chiffrez vos données et vos échanges d'information à l'aide de logiciels de chiffrement, durcissez la configuration de vos postes et utilisez des solutions de sécurité (pare-feu, antivirus). Avant d'enregistrer des fichiers à partir de supports USB, faites-les analyser (antivirus). Eteignez votre ordinateur pendant les périodes d'inactivité prolongées (nuit, week-end, vacances...). Soyez vigilant, n'évoquez pas des sujets sensibles dans les lieux publics. Enfin, utilisez des journaux d'évènements pour réagir aux phénomènes suspects : connexion hors des horaires habituels, sur un compte non actif...

3 | BÂTIR UN PLAN DE SÉCURITÉ GLOBAL

Il ne s'agit pas de tout verrouiller dans votre entreprise, mais de bâtir avec vos salariés une politique de sécurité plus globale. Elle pourra couvrir différents aspects : nommer un référent sécurité, rédiger une charte définissant les usages autorisés pour les salariés, les stagiaires, les intérimaires et les personnes extérieures à l'entreprise, gérer la sécurité de votre flotte de mobiles, tenir à jour vos installations et votre parc informatique, classer vos informations en fonction de leur degré de sensibilité, organiser un plan de continuité d'activité... Faites-vous accompagner par des spécialistes en cyber sécurité qui sauront réaliser des analyses et vous conseiller en fonction de vos besoins réels.

ALLER PLUS LOIN

- 22 fiches pratiques sur la sécurité économique - www.entreprises.gouv.fr/information-strategique-sisse/outils
- Logiciel d'autodiagnostic DIESE pour évaluer les vulnérabilités d'une entreprise et son niveau de sécurisation - www.entreprises.gouv.fr/information-strategique-sisse/outils
- ANSSI : site d'alerte et de reponse aux attaques informatiques - www.cert.ssi.gouv.fr/
- Guide des bonnes pratiques de l'informatique de l'ANSSI - www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-l'informatique
- CCI Innovation : Enquête 2015 sur les pratiques d'intelligence économique des entreprises bretonnes - innovation.bretagne.cci.fr

Pour tout renseignement,
contactez un conseiller de votre CCI
ou joignez directement au 02 99 25 41 85

Patricia Diot-Texier
Conseillère ressources humaines
patricia.diot-texier@bretagne.cci.fr

Gisèle Kermarec
Conseillère ressources humaines
gisele.kermarec@bretagne.cci.fr

un dispositif CCI BRETAGNE

PBRH+, le levier RH de la performance de votre entreprise vous propose un diagnostic, un plan d'action RH, 2 journées de formation en management et RH ainsi que 2 journées de conseils personnalisés.