LES FICHES PRATIQUES

CAMPUS RÉGION DU NUMÉRIQUE

La Région Auvergne-Rhône-Alpes

Êtes-vous bien préparé **pour votre future cyberattaque ?**

Selon une enquête de France Num, 48 % des entreprises interrogées répondent « **OUI** » à la question « **Avez-vous peur de perdre ou de vous faire pirater des données quand vous utilisez le numérique** ». Mais combien d'entre vous ont mis en place des protections ?

Que vous soyez un **indépendant**, une **TPE** ou une **PME/PMI**, nul n'est malheureusement à l'abri d'une cyber-attaque dans les semaines, mois ou années à venir. Nul ne connait la date précise mais la réflexion, à ce moment-là, sera « **J'aurais dû anticiper et le gérer avant** ».

Être capable de **maintenir son activité** et, en parallèle, de **récupérer ses données et outils informatiques** sont les éléments prioritaires pour **limiter l'impact d'une attaque**. La perte de temps, de données et souvent d'image, notamment auprès de clients ou de fournisseurs peuvent avoir un impact financier non négligeable voire fatal dans le cas d'une entreprise déjà fragile.

L'enjeu de la **cybersécurité** est donc de **protéger, en amont, son entreprise** pour limiter les risques et réduire le temps de remise en activité de l'entreprise en cas d'attaque.

FRANCE NUM

LES CCI D'AUVERGNE-RHÔNE-ALPES

ene
experts du numérique en entreprises
Auvergne-Rhône-Alpes

Check-list des protections

Nous vous proposons ce document synthétique qui vous donnera à la fois une check-list des actions à mettre en place et des pistes complémentaires pour vous aider dans votre démarche de préparation et de protection.

Je ne sais pas	Non et je ne traiterai pas ce point	Non mais je vais le traiter	Oui c'est opérationnel

CONNAISSANCE DE VOS OUTILS NUMÉRIQUES				
Connaissez-vous les données et logiciels essentiels à votre fonctionnement ?				
Maintenez-vous à jour ces systèmes ?				
Les matériels utilisés pour ces systèmes seraient-ils réparables en cas de panne ?				
SAUVEGARDE DES DONNÉES				
Sauvegardez-vous ces données ?				
Testez-vous vos sauvegardes régulièrement ?				
Etes-vous sûr que toutes vos données essentielles sont sauvegardées et restaurables ?				
VOL ET DÉGRADATION				
En cas de perte ou vol du matériel, avez-vous une solution pour redémarrer votre activité ?				
Est-ce que vous ou vos collaborateurs laissez les ordinateurs sans surveillance dans un lieu public (coffre de voiture, restaurant, train, vestiaire, ...) ?				
ASSURANCE				
Votre assurance couvre-t-elle le risque de perte ou de vol de votre matériel et de vos données ?				
Disposez-vous d'un accompagnement par un professionnel en cas de cyberattaque ?				
Etes-vous assuré pour la perte d'exploitation ?				
ANTIVIRUS / ANTISPAM				
Disposez-vous au moins d'un antivirus maintenu à jour sur chaque poste informatique (PC, serveurs, ...) ?				
Disposez-vous d'une solution antispam ? Celle-ci dispose-t-elle d'un antivirus intégré ?				
Savez-vous, ainsi que l'ensemble de vos collaborateurs, détecter un message électronique malveillant ?				
SENSIBILISATION / COMPORTEMENT DES UTILISATEURS				
Est-ce qu'une action de sensibilisation a été réalisée auprès de tous les utilisateurs ?				
Disposez-vous d'une charte informatique qui encadre l'utilisation des outils informatiques ?				
Est-ce que vous et vos utilisateurs êtes vraiment formés à l'usage des outils informatiques ?				
Formez-vous les nouveaux arrivants sur les logiciels qu'ils doivent utiliser ?				
Séparez-vous les usages privés / professionnels sur vos équipements ?				
Verrouillez-vous votre session lorsque que vous vous éloignez de votre ordinateur ?				
ORGANISATION DU RÉSEAU / FILTRAGE / ACCÈS EXTERNE				
Avez-vous mis en place un système (type pare-feu) qui n'autorise l'accès internet qu'aux services essentiels à votre activité ?				
Si vous avez des accès à distance à vos systèmes internes, utilisez-vous un VPN avec authentification personnelle de l'utilisateur ?				
Les utilisateurs doivent-ils obligatoirement utiliser un ordinateur de l'entreprise pour accéder aux données professionnelles ?				
Vos systèmes industriels sont-ils sur un réseau isolé des autres réseaux pour éviter la propagation d'une attaque sur l'outil de production ?				

SITE WEB ET E-COMMERCE				
Votre site web ou e-commerce est-il sauvegardé (fichiers et bases de données) ?				
Mettez-vous à jour régulièrement l'outil de gestion et les modules de votre site web ou e-commerce ?				
Utilisez-vous des mots de passe complexes différents des autres services ?				
Changez-vous ces mots de passe régulièrement ?				
MESSAGERIE MAIL				
Savez-vous reconnaitre un message frauduleux (hameçonnage, fichier malveillant, ...) ?				
Sauvegardez-vous votre messagerie ?				
Utilisez-vous des mots de passe complexes différents des autres services ?				
Changez-vous ces mots de passe régulièrement ?				
GESTION DES MOTS DE PASSE				
Différenciez-vous les mots de passe à usage personnel des mots de passe à usage professionnel ?				
Utilisez-vous des mots de passe complexes différents sur tous les services ?				
Changez-vous ces mots de passe régulièrement ?				
Utilisez-vous des mots de passe de complexité plus élevée pour les services sensibles ?				
Utilisez-vous un coffre-fort de mots de passe pour les stocker et les sécuriser (Keepass, LastPass, Bitwarden, ...) ?				
Lorsque cela est disponible, utilisez-vous l'authentification multifacteur (MFA) ?				
PARTAGE DE DOCUMENTS ET DE DONNÉES PERSONNELLES				
Avez-vous défini des droits d'accès aux documents sensibles partagés sur un serveur ?				
Utilisez-vous des plateformes de partage hébergées en dehors de l'Europe ?				
Avez-vous traité votre conformité au RGPD ?				
TÉLÉPHONIE MOBILE				
Vos téléphones mobiles sont-ils verrouillés avec un code d'authentification ?				
Sont-ils mis à jour régulièrement ?				
Utilisez-vous des applications qui ne seraient pas nécessaires à votre activité ?				
GESTION DE CRISE				
Savez-vous comment réagir en cas d'attaque ?				
Vous êtes-vous préparé à une crise ?				
Savez-vous comment continuer ou redémarrer votre activité en cas de crise ?				

Ce diagnostic a été élaboré par l'ENE. Il n'est pas un plan d'action.
Pour lancer votre sécurisation, retrouvez les contacts utiles en page suivante.

Les structures pour vous accompagner en région

ENE

https://www.ene.fr/

L'ENE apporte aux PME/PMI un œil d'expert sur leurs projets numériques, les aide à définir clairement leurs besoins et leur propose une méthodologie de conduite de projet.

CCI Auvergne-Rhône-Alpes

https://www.auvergne-rhone-alpes.cci.fr/

Les Chambres de Commerce et d'Industrie sont présentes aux côtés des entreprises pour les accompagner dans leur transition numérique.

Les ressources pour vous informer

Cybermalveillance.gouv.fr

https://www.cybermalveillance.gouv.fr/

Cybermalveillance.gouv.fr est une plateforme qui s'adresse à toutes les victimes d'attaques informatiques, y compris les entreprises, et qui diffuse des informations et des bonnes pratiques de prévention.

Campus Région du numérique

https://campusnumerique.auvergnerhonealpes.fr/portail-transformation-digitale/

Articles, dispositifs, tutos, guides et actus pour s'informer, s'évaluer et passer à l'action : le portail Digitalisation accompagne les entreprises dans leur transformation numérique.

Les programmes pour aller plus loin

Atouts Numériques

https://campusnumerique.auvergnerhonealpes.fr/programme-atouts-numeriques/

La Région Auvergne-Rhône-Alpes propose ce dispositif au service de la digitalisation des entreprises. Sur cette page spéciale, retrouvez les articles, les vidéos et les webinaires proposés ainsi que les informations pratiques pour bénéficier d'un accompagnement.

Industrie du Futur

https://campusnumerique.auvergnerhonealpes.fr/dispositifs/les-accompagnements-cybersecurite-pour-lindustrie/

Ce dispositif d'accompagnement des entreprises destiné aux PME et ETI de la région Auvergne-Rhône-Alpes du secteur industrie et services à l'industrie inclue un volet numérique et cybersécurité (sous réserve d'éligibilité au dispositif).

Diagnostic Cybersécurité BPI

https://www.bpifrance.fr/catalogue-offres/diagnostic-cybersecurite

Vous permet de dresser un état des lieux de l'exposition de l'entreprise aux risques cyber. Avec un expert habilité par Bpifrance, vous disposerez d'un plan d'action priorisé afin de mieux protéger son entreprise.