

## Actions prioritaires pour prévenir les cyberattaques et en réduire les conséquences

Retrouvez les bonnes pratiques pour renforcer votre sécurité numérique et anticiper la gestion d'un incident cyber sur le site de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : [Les fondamentaux pour se sécuriser | ANSSI \(cyber.gouv.fr\)](#)

Action	En quelques mots (pour une description plus précise, voir la PJ ou : <a href="#">Les Mesures Cyber Préventives Prioritaires   ANSSI</a> )
Renforcer l'authentification sur les systèmes d'information	1) Réduire au strict minimum le nombre de personnes ayant un accès « administrateur » aux outils informatiques 2) Pour tous ceux ayant un accès « administrateur » et pour l'équipe de direction, mettre en place une identification renforcée (ex : mot de passe + sms)  <a href="#">Recommandations relatives à l'authentification multifacteur et aux mots de passe   ANSSI</a>
Accroître la supervision de sécurité	En avez-vous une en place ? Il s'agit de mettre en place les outils et mesures organisationnelles pour détecter, analyser et remédier aux incidents de cybersécurité. Des prestataires de service proposent des solutions clé en mains appelées SOC (Security Operations Centers) pour assurer ces services. <a href="#">Comment déployer un SOC (clusif.fr)</a>
Sauvegarder hors ligne les données et les applications critiques pour pouvoir redémarrer votre activité	1) Sauvegarder, par exemple, sur disque dur externe déconnecté des ordinateurs évite que la sauvegarde soit elle aussi détruite par une cyberattaque 2) Vérifier, périodiquement, que la sauvegarde est réelle et utilisable (des évolutions de paramètres peuvent l'avoir rendue vide ou partielle), ç à d tester la possibilité de redémarrer à partir de la sauvegarde  <a href="#">Les règles de base de la sauvegarde   ANSSI</a> et <a href="#">Guide de la sauvegarde des systèmes d'information   ANSSI</a>
Etablir une liste priorisée des services numériques critiques de l'entité	Définir ce qui est le plus vital pour l'entreprise, ç à d ce dont la disparition serait peu remédiable et mettrait l'entreprise à plat. Pour certaines entreprises, ce sera l'ERP, pour d'autres ce seront les logiciels avec les développements en cours, etc ... <a href="#">Définir la gouvernance de sécurité numérique adaptée à son organisation   ANSSI</a>
S'assurer de l'existence d'un dispositif de gestion de crise adapté à une cyberattaque	Il s'agit pour les entreprises de définir un plan de réponse aux cyberattaques visant à assurer la continuité d'activité puis le retour à l'état nominal.  Par exemple, avez-vous défini les points de contact d'urgence, y compris chez les prestataires de service numériques, et disposez vous de leurs numéros en « version papier » ? <a href="#">Anticiper et gérer une crise Cyber   ANSSI</a>