

GUIDE DES BONNES PRATIQUES EN CYBERSÉCURITÉ



GUIDE DES BONNES PRATIQUES EN CYBERSÉCURITÉ

RÉALISÉ PAR 1FOPRESTA

03/08/2023

1

Informatif

SENSIBILISATION DU PERSONNEL

La formation et la sensibilisation de vos employés sont essentielles pour renforcer la sécurité.

2

Préventif

MISE À JOURS DES ÉQUIPEMENTS

Afin de s'assurer que les solutions techniques et opérationnelles restent pertinentes dans le temps .

3

Préventif

LIMITATION ET SURVEILLANCE DES ACCÈS UTILISATEURS

Les utilisateurs ne doivent accéder uniquement aux éléments nécessaires à la réalisation de leurs missions (permettant de cloisonner les secteurs d'activité et ainsi limiter l'impact des attaques).

4

Curatif

RÉALISATION DE SAUVEGARDES RÉGULIÈRES

Nul système n'est infailible il est important d'anticiper les méthodes de récupérations ainsi que les modalités liées afin de limiter l'impact et les conséquences d'une attaque sur l'activité de l'entreprise.



SENSIBILISATION DU PERSONNEL

La formation et la sensibilisation de vos employés sont essentielles pour renforcer la sécurité.

Organisez régulièrement des sessions de sensibilisation sur les risques de cybersécurité, les techniques d'ingénierie sociale et les bonnes pratiques à adopter en matière de mots de passe et d'accès aux données.

Changez régulièrement vos mots de passe et utilisez l'authentification multi-facteurs (AMF) lorsque possible pour une couche de sécurité supplémentaire.

MOT DE PASSE

Optez pour des mots de passe complexes et uniques pour chaque compte. Utilisez une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux, et évitez d'utiliser des informations personnelles faciles à deviner.



WWW.1FOPRESTA.COM



MISE À JOURS DES ÉQUIPEMENTS

Assurez-vous que tous vos logiciels et systèmes sont à jour avec les derniers correctifs de sécurité. Les mises à jour régulières vous protégeront contre les vulnérabilités connues.



CORRECTION DES VULNÉRABILITÉS

Les mises à jour et les patchs sont conçus pour corriger les vulnérabilités de sécurité présentes dans les logiciels et les systèmes d'exploitation utilisés par l'entreprise. En installant ces mises à jour régulièrement, l'entreprise renforce sa protection contre les cyberattaques.



PRÉVENTION DES ATTAQUES CIBLÉES

Les cybercriminels sont à l'affût des entreprises qui n'appliquent pas de mises à jour régulières. En négligeant ces mises à jour, l'entreprise devient une cible plus facile pour les attaques ciblées, telles que les ransomwares ou les logiciels malveillants.

LIMITATION ET SURVEILLANCE DES ACCÈS UTILISATEURS

La limitation et la surveillance des accès utilisateurs sont des stratégies clés pour renforcer la sécurité de votre organisation.

GESTION DES PRIVILÈGES

Il est essentiel de suivre une approche de gestion des privilèges stricte. Accordez aux utilisateurs uniquement les droits d'accès nécessaires pour effectuer leurs tâches, en évitant la surprivatisation qui pourrait exposer votre entreprise à des risques inutiles.

AUTHENTIFICATION MULTIFACTEUR

L'authentification multifacteur est un moyen efficace de renforcer la sécurité des comptes utilisateur. En plus du mot de passe, elle exige un deuxième élément d'authentification, tel qu'un code généré par une application mobile ou une empreinte digitale.

REVUE ET ANALYSE DES LOGS

La collecte et l'analyse des journaux d'activité (logs) sont essentielles pour comprendre les schémas de comportement des utilisateurs et identifier les tentatives d'intrusion.

1

**GESTION DES
PRIVILÈGES**

2

**AUTHENTIFICATION
MULTIFACTEUR**

3

**REVUE ET ANALYSE
DES LOGS**



RÉALISATION DE SAUVEGARDES RÉGULIÈRES

Effectuez des sauvegardes régulières de toutes vos données importantes. En cas de cyberattaque ou de perte de données, vous pourrez ainsi récupérer vos informations vitales sans payer de rançon.

L'OBJECTIF

L'objectif des sauvegardes régulières est de protéger et de préserver les données importantes d'une entreprise en créant des copies sécurisées et à jour de ces informations. Ces sauvegardes servent de filet de sécurité en cas de pertes de données imprévues.

1

COPIES DE SÉCURITÉ
PÉRIODIQUES

2

PRÉVENTION DES
PERTES DE DONNÉES

3

PLANIFICATION
ET AUTOMATISATION



LA CYBERSÉCURITÉ

LES ENJEUX DE LA SÉCURITÉ EN ENTREPRISE

La cybersécurité est souvent perçue comme une préoccupation majeure réservée aux grandes entités telles que les banques, les entreprises technologiques et les gouvernements.

Cependant, cette perception est trompeuse, car un nombre beaucoup plus large d'acteurs devraient se préoccuper de la cybersécurité, et pas seulement les grandes entreprises.



+400%

Une hausse de +400% de cyberattaques depuis le début de la crise sanitaire

43 %

de toutes les cyberattaques visent les petites entreprises



CYBERMENACES EN 2023

En réalité, ce sont les petites entités, comme les entreprises de moins de 1000 employés, qui sont les plus vulnérables et courent le plus grand risque en matière de sécurité informatique.

1FOPRESTA VOUS ACCOMPAGNE

1FOPRESTA dispose d'une équipe d'experts en cybersécurité hautement qualifiés et expérimentés. Ils sont en mesure d'analyser les vulnérabilités de votre infrastructure informatique, d'identifier les risques potentiels et de mettre en place des stratégies de défense robustes pour protéger vos données et systèmes sensibles.

EXPERTISE EN CYBERSÉCURITÉ

1FOPRESTA est composée de professionnels hautement expérimentés et qualifiés, cumulant plus de 20 ans d'expertise.

SOLUTIONS SUR MESURE

1FOPRESTA propose des solutions sur mesure adaptées aux besoins spécifiques de votre entreprise.

SURVEILLANCE ET RÉACTIVITÉ

1FOPRESTA assure une surveillance proactive de votre environnement informatique afin de détecter rapidement toute activité suspecte ou tentative d'intrusion.

SENSIBILISATION ET FORMATION

Outre la mise en place de mesures de sécurité avancées, 1FOPRESTA propose également des programmes de sensibilisation et de formation pour vos employés.



L'informaticien des entreprises

WWW.1FOPRESTA.COM



PARIS / ILE DE FRANCE : 01 84 16 78 10

SAINT-MALO / BRETAGNE : 02 57 64 00 64

AIX-EN-PROVENCE / PACA : 04 84 49 20 50