Cyberdefense

Chef de Produits

Les bons gestes recommandés par UrgenceCyber

5 GESTES DE PRÉVENTION CONTRE LES CYBERATTAQUES

1 LIMITEZ LES ACCÈS AUX DONNÉES SENSIBLES

Vos employés ne doivent accéder qu'aux informations dont ils ont besoin pour effectuer leurs missions. Les accès doivent être régulièrement examinés et résiliés si nécessaire.

2 UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

Celui-ci permet de stocker et générer automatiquement tous vos mots de passe. Privilégiez le logiciel KeePassXC, qui est 100% gratuit et certifié par l'ANSSI.

3 MAINTENEZ VOTRE SYSTÈME D'EXPLOITATION À JOUR

La mise à jour de vos réseaux, vos pares-feux, vos antivirus et vos logiciels permet d'améliorer significativement le niveau de sécurité de vos systèmes contre les cyberattaques.

4 PENSEZ À SAUVEGARDER RÉGULIÈREMENT VOS DONNÉES

Cette pratique permet de protéger vos données des actes malveillants. Les sauvegardes peuvent être enregistrées sur divers supports : le cloud, une clé USB, un disque dur ou encore un serveur de stockage en réseau.

5 SENSIBILISEZ VOS SALARIÉS AUX RISQUES CYBER

Informez-les des bonnes pratiques en matière de sécurité informatique. Aidez-les à identifier les menaces et formez-les sur les actions à mener en cas de cyberattaque.

En cas d'attaque cyber, n'hésitez pas à appeler le 0 800 730 647. Les analystes d'Urgence Cyber IDF se tiennent à votre écoute afin de résoudre vos incidents au plus vite.

COMMENT BIEN SAUVEGARDER VOS DONNÉES ?

1 CRÉEZ UN PLAN DE SAUVEGARDE

Répertoriez et catégorisez vos différents types de données (data, logiciels, applications...). Votre plan doit notamment définir les durées de rétention et préciser la répartition à long terme, par exemple : 15 jours de sauvegardes journalières, 1 an de sauvegardes mensuelles et 5 ans de sauvegardes annuelles.

2 APPLIQUEZ LA RÈGLE "3-2-1"

Elle consiste à effectuer 3 copies de la sauvegarde sur 2 supports différents dont **1 hors ligne. Celle-ci est indispensable car si votre entreprise subit un incident, vous ne perdrez pas vos données.**

3 DÉFINISSEZ UNE STRATÉGIE ET UN ORDRE DE RESTAURATION

Ces derniers doivent tenir compte des critères suivants : dépendance du SI vis-à-vis de services d'infrastructure (DNS, NTP, annuaire...), criticité des applications métier, durée de restauration et de resynchronisation des données et mode de restauration.

4 TESTEZ RÉGULIÈREMENT VOS SAUVEGARDES

Une sauvegarde et une restauration doivent être testées en contexte normal afin de s'assurer de leur bon fonctionnement.

5 QUE FAIRE EN CAS D'INCIDENT ?

Si vous êtes victime d'un incident de sécurité, la mesure prioritaire est d'isoler l'infrastructure de sauvegarde du reste du système informatique. A cet effet, prévoyez un mode "bouton rouge" d'urgence (déconnexion d'un commutateur, script automatisé...).

En cas d'attaque cyber, n'hésitez pas à appeler le 0 800 730 647. Les analystes d'Urgence Cyber IDF se tiennent à votre écoute afin de résoudre vos incidents au plus vite.

5 GESTES DE PREMIERS SECOURS CONTRE LES ATTAQUES CYBER

1 N'ÉTEIGNEZ PAS VOTRE APPAREIL

N'éteignez pas votre appareil et n'utilisez plus l'équipement potentiellement compromis. La machine doit être maintenue sous tension afin d'identifier les processus actifs.

2 DÉCONNECTEZ LA MACHINE DU RÉSEAU

Isolez immédiatement tous les systèmes concernés du réseau pour stopper l'attaque. Le hacker ne pourra plus récupérer, consulter ou modifier les fichiers de votre organisation.

3 ALERTEZ VOTRE SUPPORT INFORMATIQUE

Prévenez immédiatement votre service informatique, vos collègues de travail ainsi que toutes les sociétés partenaires susceptibles d'être impactées par la cyberattaque. Pensez également à changer tous vos mots de passe.

4 AVERTISSEZ LES AUTORITÉS COMPÉTENTES

Portez plainte le plus rapidement possible auprès de la police ou de la gendarmerie. Si vous êtes victime d'une fraude bancaire, signalez la sur la plateforme Perceval et déclarez le sinistre auprès de votre assureur.

5 RÉCUPÉREZ LES TRACES DE L'INTRUSION

Enregistrez toutes les preuves (logs, pares-feux, copie complète du PC...) de l'attaque informatique et désignez un collaborateur chargé de tenir un registre regroupant les événements et actions réalisées.

En cas d'attaque cyber, n'hésitez pas à appeler le 0 800 730 647. Les analystes d'Urgence Cyber IDF se tiennent à votre écoute afin de résoudre vos incidents au plus vite.

Des partenaires sur le territoire pour vous accompagner

orange™ Cyberdefense est là

Contacts : 3901 / Boutiques
orangecyberdefense.com/fr/

frederic.lejan@orange.com

SEINE-ET-MARNE NUMÉRIQUE

Offre de services :
- Sensibiliser votre collectivité
- Comprendre et évaluer les risques cyber
- Cyber assurance
- Sauvegardes externalisées

servicesnumeriques@seineetmarnenumerique.fr

CCI SEINE-ET-MARNE

#SecNumEco 2024
SecNumEco 2024 - CCI Seine-et-Marne

Offre de services :
- des évènements
- de nombreuses formations
- des informations disponibles

Conseiller numérique expert en sécurité de l'information : sgauduchon@seineetmarne.cci.fr

Région îledeFrance
POUR GAGNER ensemble

Plateforme d'assistance cyber :

0800 730 647 - urgencecyber.iledefrance.fr

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

Plateforme Info Escroqueries du ministère de l'Intérieur au :

0805 805 817 - cybermalveillance.gouv.fr

COMMANDEMENT ZONAL
GENDARMERIE ÎLE-DE-FRANCE

di@G@Nal

cybergend77@gendarmerie.interieur.gouv.fr
0164717124 et le 17