Prévention CYBER ÉTÉ 2024

Ne laissez pas Les Grands Évènements Sportifs mettre votre entreprise hors jeu

Les cybercriminels ne font pas de distinction entre grandes entreprises et PME : toute organisation connectée est une cible potentielle.

En 2020, malgré des gradins vides, Tokyo a été la cible de 450 millions de cyber attaques et a dû parer à des menaces, déjà un chiffre vertigineux.

À l'approche des grands évènements sportifs de l'été, les estimations font état d'un chiffre de **8 à 10 fois supérieur**. Le risque d'une cyberattaque impactant indirectement votre entreprise n'a jamais été aussi élevé.

Selon l'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI), **69 % des cyber attaques visaient des entreprises depuis 2020.**

Les cyber attaques visent principalement les TPE / PME / ETI.
45 % d'entre elles ont fait l'objet d'une attaque en 2023
(Source : baromètre CESIN 2023)

Vous pourriez être la victime collatérale, alors ne laissez pas votre entreprise devenir une statistique.

Comment faire pour éviter cela ? Un guide pratique (Guide BPI France)

Sensibilisez vos collaborateurs

80 % des attaques démarrent par un mail de phishing. Il est donc crucial de sensibiliser vos collaborateurs de façon régulière :

- Reconnaître les tentatives de phishing,
- Créer un mot de passe robuste,
- Assurer la confidentialité des données…

Mettez à jour vos appareils, vos logiciels et vos antivirus

- Assurez-vous que tous les équipements, logiciels et programmes utilisés par votre entreprise soient régulièrement mis à jour avec les derniers correctifs de sécurité.
- Maintenez à jour tous les équipements, logiciels, applications, antivirus avec les derniers correctifs de sécurité.

Gérez vos mots de passe

- Un mot de passe robuste doit comporter au minimum 12 caractères mélangeant majuscules, minuscules, chiffres et caractères spéciaux.
- Il doit être changé régulièrement.
- Encouragez l'utilisation de gestionnaires de mots de passe.
- Activez l'authentification multifacteurs dès que cela est possible.

Évitez les comportements à risque

- N'ouvrez pas de pièce jointe suspecte ou provenant d'un expéditeur inconnu.
- Évitez de brancher une clé USB trouvée en apparence abandonnée, car elle pourrait avoir été intentionnellement placée pour piéger une victime potentielle. Avant de cliquer sur un lien, vérifiez le nom de domaine en passant votre souris dessus, et évitez les sites douteux.
- En déplacement, évitez d'utiliser le wifi public.
- Séparez les usages professionnels et privés de vos appareils.
- Soyez vigilant à votre e-réputation sur les réseaux sociaux.

Sauvegardez

Les sauvegardes sont un élément essentiel de sécurité :

- Sauvegardez régulièrement les données essentielles aux activités de l'entreprise sur au moins un support déconnecté du réseau.
- Idéalement, disposez d'une copie de sauvegarde chiffrée.
- Effectuez régulièrement un test de restauration.

Mettez en place des garde-fous

Les prérequis :

- Antivirus et Pare feu activés en permanence

Implémentez des mesures de sécurité supplémentaires :

- VPN pour les accès distants
- Solution de détection d'intrusion

Que faire en cas d'attaque ?

1. Alertez immédiatement votre support informatique et votre assureur.
2. Isolez les systèmes attaqués.
3. Constituez une équipe de gestion de crise.
4. Préservez les preuves de l'attaque et portez plainte dans les 72 heures.

Renseignez-vous au préalable sur la disponibilité de votre support informatique durant l'été

AXA Prévention

La Prévention, meilleure arme contre les cyberattaques

Vous souhaitez aller plus loin

ACYMA (Site gouvernemental contre la cybermalveillance)

ANSSI (Agence nationale de la sécurité des systèmes d'information)

Ma Brigade Numérique

Cybersécurité : un guide pratique (Guide BPI France)

Ref 20052360 4 2024 - Solutions Graphiques - Crédit photo : Adobe Stock