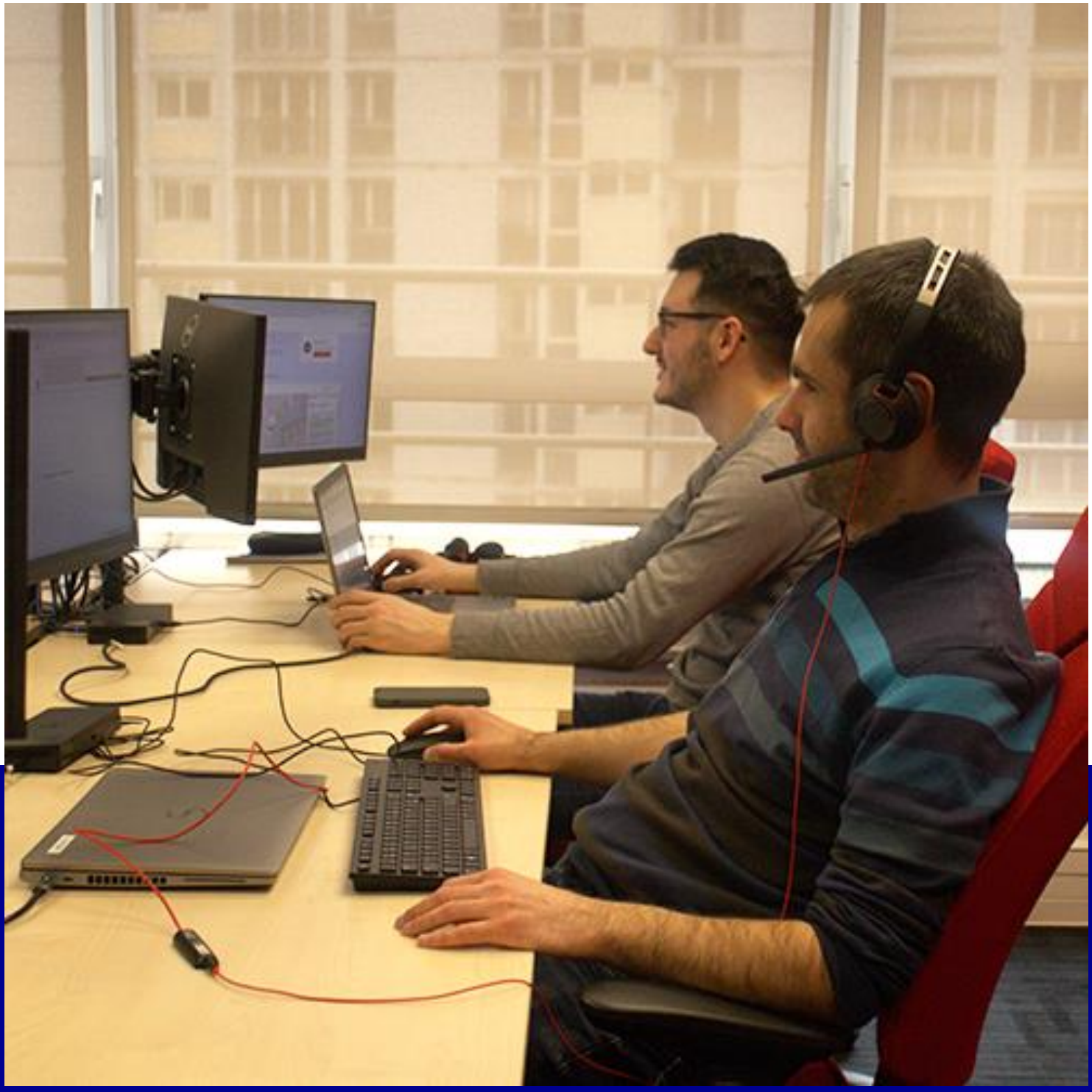
Dossier de presse
À la rencontre d'Urgence Cyber Île-de-France



Région îledeFrance

Sommaire

Le risque de défaillance d'une PME augmente de 50 % dans les 6 mois qui suivent une attaque cyber ! Mais la perception de la menace reste sous-estimée avec encore un quart des entreprises considérant le risque cyber inexistant. C'est la raison pour laquelle la Région Île-de-France agit pour sensibiliser et accompagner les PME franciliennes mais aussi nos collectivités face à ces risques croissants.

La plateforme Urgence Cyber Île-de-France est l'un des derniers outils que nous avons mis en place pour les petites et moyennes entreprises, en lien avec l'Anssi : cette plateforme gratuite d'assistance face à la menace cyber, répond aux situations d'urgence et fournit une aide de premier niveau afin de vous accompagner et vous mettre en relation avec des prestataires cyber labellisés. N'hésitez pas à vous en saisir !

Alexandra Dublanche, vice-présidente du Conseil Régional Ile-de-France, chargée de la Relance, de l'Attractivité, du Développement économique et de l'Innovation

Région îledeFrance

Qui sommes-nous ?

Un centre de réponse aux cyberattaques

Pour faire face à l'accroissement de la cybermenace, la Région Ile-de-France, a créé, avec le soutien de l'Etat et de l'agence nationale de la sécurité des systèmes d'information (ANSSI), un centre de réponse aux incidents cybersécurité, Urgence Cyber Île-de-France, dédié aux entreprises, aux associations et aux collectivités franciliennes.

Nos missions

La mission d'Urgence Cyber Île-de-France consiste à délivrer une première réponse aux entreprises, associations et collectivités franciliennes victimes de cyberattaques ou d'incidents de sécurité numérique. En cas d'urgence, elle offre un accompagnement en proximité :

- Apporter une assistance d'urgence personnalisée via un centre d'appel,
- Etablir un diagnostic à distance,
- Informer et conseiller sur les gestes de premiers secours et les actions à mener,
- Répondre à la nature de l'incident et mobiliser d'un prestataire spécialisé si nécessaire,
- Accompagner dans les démarches juridiques à engager.

Urgence Cyber Île-de-France sensibilise également l'écosystème régional à la cybersécurité à travers des dispositifs de sensibilisation gratuits (ateliers, conférences, webinaires, démonstrations d'attaques…).

Urgence Cyber
îledeFrance
0 800 730 647
Appel gratuit

Contact

Urgence Cyber Île-de-France

urgencecyber@iledefrance.fr

0 800 730 647

Quelques chiffres sur la cybersécurité

50%

des entreprises ont été victimes d'une attaque informatique en 2023

385 000

cyberattaques réussies à l'encontre des entreprises françaises en 2022 (dont 86% visant les PME)

91%

des organisations touchées par des cyberattaques identifient le phishing comme 1er vecteur d'attaque

40%

des petites et moyennes entreprises (PME) ont été victimes d'un rançongiciel

50%

Le risque de défaillance d'une PME augmente de 50% dans les 6 mois qui suivent une attaque cyber

339M€

levés en cybersécurité en France en 2022. En Europe, la France arrive en 3ème position après la Suisse et le Royaume-Uni

Région îledeFrance

Un service en 24/7 pendant la période des JOP

Un climat propice aux cyberattaques

En raison de leur portée médiatique internationale, les Jeux Olympiques et Paralympiques de Paris 2024 sont susceptibles d'attirer l'attention d'un grand nombre d'acteurs cyber malveillants. On estime qu'il y aura 8 à 10 fois plus d'attaques informatiques enregistrées qu'en 2021 (soit plus de 4 milliards en 2024 contre 450 millions lors des Jo de Tokyo).

Dans ce contexte, Urgence Cyber Île-de-France fonctionne en 24/7 du 12 juillet au 12 août pour résoudre les incidents cybers franciliens le plus efficacement possible.

Des prestataires techniques de confiance

Pour aider les victimes de cyberattaque, nous proposons systématiquement de les mettre en relation avec des experts cyber choisis par nos soins, ce qui leur confère un gain de temps considérable dans la résolution finale de l'incident. Nous avons 15 prestataires à disposition dont Orange Cyberdefense, Almond ou encore Intrinsec.

Bonnes pratiques cyber

Consultez nos 3 infographies sur les bonnes pratiques cyber (pages 9, 10 et 11).

Urgence Cyber îledeFrance

Région îledeFrance

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.

Urgence Cyber Île-de-France

Région îledeFrance

COMMENT BIEN SAUVEGARDER VOS DONNÉES ?

1 CRÉER 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.

Urgence Cyber îledeFrance

Région îledeFrance

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.