FICHE CLIENT

ORECC

VOUS INFORME

Avril 2022

RISQUE CYBER AU REGARD DE L'ENVIRONNEMENT GEOPOLITIQUE

Nous faisons face à de nombreuses tensions géopolitiques, dont les effets sur la cybersécurité sont à anticiper. Quelle que soit l'activité de votre entreprise, nul n'est épargné par le risque cyber au regard du contexte international.
Nous attirons donc votre attention sur la nécessité de renforcer votre vigilance et de mettre en œuvre des mesures de cybersécurité pour garantir la protection de votre entreprise.

Les 5 mesures cyber-préventives prioritaires de l'ANSSI

L'Agence de cybersécurité civile française (ANSSI) incite les entreprises à mettre en œuvre les 5 mesures préventives prioritaires ci-dessous afin de limiter la probabilité d'une cyberattaque ainsi que ses potentiels impacts :

1. Renforcer l'authentification sur les systèmes d'information
2. Accroître la supervision de sécurité
3. Sauvegarder hors-ligne les données et les applications critiques
4. Établir une liste priorisée des services numériques critiques de l'entité
5. S'assurer de l'existence d'un dispositif de gestion de crise adapté à une cyberattaque

Nous vous invitons à télécharger le support publié sur le site de l'ANSSI ci-après : https://www.ssi.gouv.fr/uploads/2022/02/20220226_mesures-cyber-preventives-prioritaires.pdf

Alertes et avis de sécurité émis par le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR)

L'ANSSI préconise également de consulter régulièrement et attentivement les avis de sécurité émis par le CERT-FR afin de prévenir d'un éventuel danger :
https://www.cert.ssi.gouv.fr/

Guide d'hygiène informatique de l'ANSSI

Pour aller plus loin, il est recommandé de vous assurer de la bonne mise en place des mesures de sécurité présentées dans le guide d'hygiène informatique de l'ANSSI pour renforcer la sécurité de votre système d'information.

Bons réflexes pour se prémunir du phishing

Le phishing (ou hameçonnage) consiste à escroquer en ligne en envoyant de faux courriels imitant ceux d'une institution ou entreprise et semblant provenir d'une source fiable.

Pour vous prémunir de ce type de campagne d'attaques, il est recommandé de redoubler d'attention pour avoir un comportement responsable et avisé. Il s'agit en effet de faire preuve de bon sens, garder un esprit critique, ne jamais se précipiter, et prendre toujours le temps de la réflexion en cas de réception de courriel douteux.

Ci-dessous les réflexes incontournables à adopter pour protéger son système d'information d'une éventuelle attaque :

LA CYBERSÉCURITÉ EST PLUS QUE JAMAIS L'AFFAIRE DE TOUS.

NOUS VOUS REMERCIONS DE VOTRE VIGILANCE ET VOUS ASSURONS DE NOTRE ENGAGEMENT POUR LUTTER ENSEMBLE CONTRE LA CYBERCRIMINALITÉ