PRÉFET
DE LA MOSELLE
Liberté
Égalité
Fraternité

Cabinet
Direction des sécurités
Pôle sécurité intérieure

Metz, le 2 mars 2022

Addendum - POSTURE VIGIPIRATE

VIGIPIRATE
SECURITE RENFORCEE
RISQUE ATTENTAT

En application du plan VIGIPIRATE l'ensemble du territoire national est maintenu au niveau « sécurité renforcée-risque attentat »

La nouvelle posture Vigipirate « hiver 2021 - printemps 2022 » qui vous a été transmise le 6 janvier 2022 fait l'objet d'un addendum à la suite de l'offensive des forces armées russes en Ukraine. Dans un contexte de fortes tensions diplomatiques, de menaces terroristes et sanitaires persistantes, il convient d'adapter notre posture de sécurité globale pour réduire les vulnérabilités liées à cette situation inédite.

Le Premier ministre a décidé d'activer des mesures du plan VIGIPIRATE de protections supplémentaires tout particulièrement dans le domaine numérique :

- **NUM 31-06** : sensibiliser les utilisateurs sur un risque de sécurité et un comportement à adopter.

En effet, les collaborateurs des entreprises et des administrations peuvent être la cible de campagne de hameçonnage ciblé en particulier les utilisateurs disposant de droits étendus sur les systèmes d'informations (administrateur technique ou fonctionnel).

Dans ce contexte, il est important de s'assurer de la bonne mise en place des mesures d'hygiène informatique essentielles présentées dans le guide d'hygiène informatique de l'ANSSI (https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf), en particulier les actions visant à améliorer la sensibilisation des utilisateurs sur l'identification des risques de sécurité et des bons comportements à adopter.

De fait, une vigilance accrue doit être portée sur les trois points suivants :

1- *concernant la messagerie électronique*

-appliquer rigoureusement les consignes de sécurité concernant les spams et les messages douteux ;
-ne pas ouvrir des messages provenant d'adresses inconnues ;
-ne pas ouvrir des pièces jointes douteuses ;
-ne pas cliquer sur des liens électroniques incertains ;
-signaler les messages malveillants ;

2- *concernant la transmission de documents*

-privilégier les outils sécurisés de partage de documents plutôt que l'envoi (en pièces jointes) par messagerie électronique ;

3- *en cas d'erreur de traitement de messages malveillants ou/et de fonctionnement anormal de votre équipement numérique (ordinateur de bureau ou portable, smartphone)*

-alerter immédiatement l'équipe SSI de la structure ;

- **NUM 21-02** : consulter régulièrement les sources d'information relatives aux vulnérabilités et attaques notamment le site internet du centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR).

L'ANSSI publie les alertes de sécurité devant être prises en compte par les entreprises et les administrations en indiquant le niveau d'urgence et les actions à mener. Ces alertes et avis sont centralisés sur le site CERT-FR :

-https://www.cert.ssi.gouv.fr/alerte/
-https://www.cert.ssi.gouv.fr/avis/

Le Premier ministre a par ailleurs décidé d'activer la mesure du plan PIRANET :

- **NET 2-1-1** : superviser en temps réel l'état de disponibilité des éléments des systèmes d'information.

Les tensions internationales actuelles, notamment entre la Russie et l'Ukraine, peuvent parfois s'accompagner d'effets dans le cyberespace qui doivent être anticipés. Dans ce contexte, la mise en œuvre des mesures de cybersécurité et le renforcement du niveau de vigilance sont essentielles pour garantir la protection au bon niveau des organisations. Les entreprises et les administrations doivent surveiller les comportements anormaux sur les systèmes d'information en particulier en lien avec les alertes publiés par le CERT-FR : https://www.cert.ssi.gouv.fr/

*

En cas de dysfonctionnements constatés, sans attendre d'avoir caractérisé l'origine du dysfonctionnement (panne ou attaque), les opérateurs et les administrations sont invités à en informer le cert-fr.cossi@ssi.gouv.fr

Le préfet,

Laurent Touvet