ANNEXE

Mesures nouvellement activées

1 Domaine numérique

1.1 Mesures du plan *VIGIPIRATE*

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

Dans le cadre des tensions internationales actuelles, les collaborateurs des entreprises et des administrations peuvent être la cible de campagne de hameçonnage ou d'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

Mesure (NUM 21-02) : consulter régulièrement les sources d'information relatives aux vulnérabilités et attaques (site Internet du 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 du CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) https://www.cert.ssi.gouv.fr/alerte/ et https://www.cert.ssi.gouv.fr/avis/

Les entreprises et les organisations sont invitées à consulter régulièrement ces sources et appliquer les mesures associés.

1.2 Mesure du plan *PIRANET*

Mesure (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. Si aucune cybermenace visant les organisations françaises en lien avec les récents événements n'a pour l'instant été détectée, il est nécessaire de suivre la situation de près. 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. Nous incitons donc les entreprises et les administrations à 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 dysfonctionnement 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