Note / 20	Correcteur

Épreuve de Note de synthèse

N° d'anonymat (4)
6754

Feuille n° 1 / 1 (5)

NOTE

à l'attention de
Monsieur le chef de cabinet

Objet : Le défi de la mise en œuvre d'une politique publique d'accompagnement de la société française vers la cyber résilience

En 2021, l'Agence nationale de sécurité des systèmes d'information (ANSSI) relevait 1082 intrusions avérées dans des systèmes d'information, soit une hausse de 37 % par rapport à 2020.

Si le processus de transition numérique de la société française semble irréductible face à l'évolution des besoins et des usages, il a pour corollaire une vulnérabilité accrue de l'ensemble des acteurs face aux cybermenaces, d'où le caractère crucial de la mise en œuvre d'une politique publique d'accompagnement vers la cyber-résilience.

Face à la multiplication des menaces (I) de multiples actions ont été engagées pour protéger les acteurs (II) et devront être approfondies pour conforter la cyber-résilience de la Nation (III).

146

I/ La multiplication des menaces, conséquence d'une transition numérique irréductible.

Si la transition numérique a vocation à faciliter les démarches des citoyens ainsi que des organismes publics et privés, elle a pour corollaire une vulnérabilité accrue

(1) Indiquer la nature du concours.
(2) Précisez le niveau : CME - CM1 - CM2 - CTE - CT1 - CT2 - CT1/VE - CAT2 - BSAT - BSTAT.
(3) Pour les examens de langues, préciser : active, réserve, service détaché.
(4) Ne rien inscrire dans cette case.
(5) Le candidat porte au numérateur le numéro d'ordre de la feuille et au dénominateur le nombre total de documents constituants sa composition (ex. : 1/3 puis 2/3 et 3/3).

ÉDIACA SAINT-ÉTIENNE - 2013060041
SGA/SPAC/PGT Impressions

des usagers du numérique face aux cyberattaques.

• Le développement de "l'e-administration" qui consiste en l'utilisation des technologies de l'information et de la communication pour améliorer la gestion des affaires publiques accroit la quantité de données personnelles disponibles en ligne et in fine le risque de vol de données. À cet égard, le programme Action publique 2022 aboutira à la dématérialisation des 250 démarches administratives les plus courantes.

• Par ailleurs, la multiplication des usages du numérique suite à la pandémie s'est traduite par une recrudescence des cyberattaques contre lesquelles les entreprises sont plus ou moins bien armées. Contrairement aux grands groupes, les TPE, PME et ETI sont plus susceptibles d'être victimes de demandes de rançon ou de mise à l'arrêt de leurs équipements.

• Enfin, les grandes infrastructures administratives de l'Etat, telles que les collectivités territoriales et les hôpitaux, sont menacées par l'installation de logiciels du type cheval de Troie. À l'image de l'attaque du centre hospitalier de Versailles en décembre 2022, la désorganisation créée par des attaques coordonnées peut rendre indisponibles des services publics élémentaires.

364

II/ De multiples actions engagées pour assurer la résilience de la Nation.

De nombreuses actions ont d'ores et déjà été engagées par l'Etat en matière de sensibilisation et de sécurisation auprès des acteurs publics et privés.

• Les TPE, PME et ETI, particulièrement exposés, font l'objet de mesures spécifiques. Le ministre délégué à la transition numérique a ainsi annoncé l'octroi d'un

budget de 30 millions d'euros dédié à l'activation d'un "bouclier cyber" au sein des entreprises relevant de secteurs critiques. En outre, Bpifrance s'est associé au dispositif cybermalveillance.gouv.fr pour produire un guide de bonnes pratiques et développer la "cyber hygiène" au sein des entreprises.

· Concernant l'Etat, les collectivités territoriales et les établissements de santé, l'élévation durable de leur niveau de cybersécurité a été initiée dans le cadre du plan France Relance. L'ANSSI bénéficie pour cela d'une enveloppe de 136 millions d'euros dont 60 millions destinés aux collectivités territoriales pour la création de centres régionaux de réponse à des incidents cyber.

· Enfin, le gouvernement a prévu la mise en place d'outils à destination des particuliers. Il s'agira d'un filtre visant à avertir les internautes qui naviguent sur un site malveillant ainsi que de l'affichage d'un "cyber score" indiquant le niveau de protection des données garanti sur chaque site internet.

589

III / Des leviers d'action à exploiter pour renforcer la cyber-résilience.

Compte tenu de la prégnance des risques cyber, il apparait nécessaire de renforcer les bonnes pratiques et les moyens alloués à la cyber-résilience.

1- Développer une véritable cyberculture au sein de la population par une politique de sensibilisation dès le plus jeune âge.

Alors que 72 % des Français n'ont jamais reçu de formation cyber (enquête IPSOS et TerraNova), 78 % des jeunes de 13 à 19 ans sont inscrits sur les réseaux sociaux sans en maîtriser les dangers. D'où l'importance de poursuivre la sensibilisation du grand public.

689

2- Généraliser les bonnes pratiques en matière de cybersécurité au sein des structures publiques et privées.

Cela induit la mise en œuvre d'une politique de management des risques cyber par l'élaboration d'une cartographie des risques intégrée au sein du contrôle interne, des audits réguliers et l'identification d'un référent pour la sécurité des systèmes d'information de chaque organisme.

3- Renforcer les moyens technologiques et humains alloués à la cyberdéfense dans le cadre de la loi de programmation militaire 2024-2030.

Dans un contexte marqué par le retour de la haute intensité, la cyberdéfense participe plus que jamais à la cyber-résilience de la Nation. Aussi, un effort budgétaire devra être fourni afin de renforcer les capacités opérationnelles du Comcyber (commandement de la cyberdéfense).

815

Au regard du renouvellement des menaces, lesquelles ne sont plus seulement matérielles et concernent potentiellement chaque citoyen, que ce soit dans ses usages privés ou professionnels du numérique, la question de la cyber-résilience apparaît plus que jamais centrale. La politique publique d'accompagnement de la société française vers la cyber-résilience devra permettre d'en conforter les cinq piliers : identifier, protéger, détecter, répondre et récupérer. L'organisation des Jeux Olympiques en France constituera à cet égard un défi de taille et une évaluation en temps réel de l'état de la cyber-résilience de la Nation.

Nombre de mots : 913.