Note / 20	Correcteur

Épreuve de Note de synthèse

N° d'anonymat (4)
0297

Feuille n° 1 2 (5)

Note à l'attention de monsieur le ministre délégué chargé de la transition numérique et des télécommunications

Objet : Mise en place d'une politique publique de cybersécurité

L'irruption en 2020 de la crise de la COVID-19 a été un moment de réalisation de l'accroissement de notre dépendance collective aux outils numériques. Cela est notamment dû à la transition numérique entamée par le secteur public à la fin des années 1990 et qui a aujourd'hui abouti, à la suite de programmes comme PAGSI et action publique 2022, à la possibilité pour les administrés de réaliser près de 250 démarches administratives de façon entièrement dématérialisée. Le secteur privé n'est ici pas en reste, le numérique étant un outil privilégié par les entreprises pour leur développement, que ce soit par les gains de productivité permis ou par la création de nouveaux biens et services.

Cet accroissement du volume de la sphère numérique publique comme privée conduit mécaniquement à une augmentation du nombre des cibles potentielles de cyber attaque. De ce fait ces attaques sont appelées à se multiplier et toutes ne pourront être empêchées. Il paraît donc judicieux de basculer d'une logique

(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

de cybersécurité à une logique de cyberrésilience, permettant une approche intégrant la cybersécurité, la gestion de crise et la capacité à se relever d'une cyber.

Se pose alors la question de savoir comment réussir à mettre en place une politique publique cohérente d'accompagnement de la société française vers la cyberrésilience. Pour cela, la présente note exposera la diversité des cybermenaces actuelles (I) ainsi que des actions entreprises pour les contrer (II) avant de proposer des axes de réflexion pour renforcer la cyberrésilience de la société française (III).

I/ La diversité des cybermenaces actuelles

Les premières menaces venant à l'esprit sont celles pesant sur les capacités d'action et de fonctionnement des administrations et des entreprises. Ces menaces se manifestent le plus souvent sous la forme d'attaques DDOS, visant à nuire purement et simplement à l'institution visée, et de ransongiciels visant à extorquer des fonds à la victime. Dans le secteur privé plus de 10 000 entreprises se sont déclarées victime de ce genre d'attaques en 2020, la majorité étant des PME qui, du fait de leur faible taille, sont particulièrement fragiles face à ces menaces. Pour le secteur public 2020 a également marqué une augmentation du nombre d'attaques contre les collectivités territoriales.

Un autre pan qu'il ne faut pas sous estimer des cybermenaces concerne celles pesant sur les données personnelles des individus.

En effet, la transition numérique s'accompagne d'un partage croissant de données personnelles qui constitent autant de cibles pour des pirates, 76% des salariés français, britaniques, canadien, australien et américains se déclarent victime de cyberattaque ou connaissant une personne victime de cyberattaque. Cela est d'autant plus problématique que 62% des français n'ont jamais reçu une formation à la cybersécurité.

Le dernier groupe de menaces à souligner concerne celles relatives au domaine de la défense. Les infrastructures de défense sont de plus en plus exposées à des cyber attaques, notamment de par leur recours accru aux outils informatiques et leur intégration à des systèmes de combat. L'attaque subit le 24 février 2022 par les forces armées ukrainiennes et visant leur réseau de communication en est un exemple récent.

II/ Des réponses s'organisant à plusieurs niveaux

Pour ce qui est des mesures mises en place pour le secteur privé il s'agit de la création récente d'un "bouclier cyber" doté d'un fonds de 30 millions d'euros et destiné à accompagner les PME, entreprises les plus touchées, vers une amélioration globale de leur cyber résilience. A cela s'ajoute l'action de plusieurs services de l'Etat, dont cybermalveillance.gouv.fr, pour produire des guides pratiques à destination du secteur privé pour leur permettre de renforcer leur cybersécurité.

Le pendant destiné au secteur public de cet effort passe par la mise en place par

l'ANSSI, dans le cadre du plan France relance, d'un plan à destination des structures de l'Etat et des collectivités territoriales, visant à mettre en place des parcours de sécurité des systèmes d'information ainsi que par la création de centres régionaux de réponse à des incidents cyber. Pour ce faire l'ANSSI dispose d'une enveloppe de 136 millions d'euros sur la période 2020-2022.

La mise en place d'actions d'accompagnement vers la cyber résilience ne peut se faire à une échelle uniquement nationale. L'Union européenne a, par le biais du Conseil de l'Union européenne, adopté en 2021 plusieurs conclusions en matière de cybersécurité comprenant notamment la mise en place d'une unité conjointe de cybersécurité. L'Union européenne a également embrassé le concept de cyber résilience avec l'annonce récente, par la commission, d'un projet de règlement européen intitulé "Cyber Resilience Act" et proposant l'édiction d'obligations supplémentaires pour les fabricants de matériels et de logiciels informatiques.

III / Propositions

L'état des menaces cyber et des actions mises en place pour les contrer ayant été posé, les propositions visant à continuer l'accompagnement de la société française vers la cyber résilience sont les suivantes :

1- Mettre en place un plan de formation initiale et continue visant à sensibiliser le public aux enjeux et bonnes pratiques en

Note / 20	Correcteur

Épreuve de Note de synthèse

N° d'anonymat (4)
0297

Feuille n° 2/2 (5)

matière de cyber sécurité. Cela passerait par l'intégration d'un volet cybersécurité à l'outils de formation et de certification des compétences informatique PIX et qui serait intégré au cursus de tous les élèves du secondaire. Cela serait accompagné par la formation des actifs via la formation continue à ces même enjeux, par nature en perpetuelle évolution.

2- Renforcer humainement et matériellement les structures publiques en charge du cyber (ComCyber, ComCybergend et ANSSI), leur permettant de mieux traiter la masse croissante d'incidents les concernant et leur permettant d'adopter une attitude proactive d'anticipation des menaces et de développement des parades associées;

3- Inciter, voire obliger, les institutions publiques et les entreprises à se doter de plan de contingence anticipant les conséquences possibles de cyberattaques et prévoyant les modalités appropriées de continuation de leur activité, permettant ainsi de minimiser l'impact négatif des attaques susmentionnées.

862 mots

(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