EXAMEN PROFESSIONNEL D'AVANCEMENT DE GRADE DE TECHNICIEN PRINCIPAL TERRITORIAL DE 2ème CLASSE

SESSION 2023

ÉPREUVE DE RAPPORT AVEC PROPOSITIONS OPÉRATIONNELLES

ÉPREUVE D'ADMISSIBILITÉ :

L'épreuve d'admissibilité consiste en la rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt.
Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGENIERIE, INFORMATIQUE ET SYSTEMES D'INFORMATION

INDICATION DE CORRECTION

Sujet :

Vous êtes technicien principal territorial de 2ème classe, en poste en qualité de responsable sécurité des systèmes d'information (R.S.S.I.), en charge de la direction informatique de la commune de Techniville (10 000 habitants).

Des communes voisines ont récemment été victimes de cyberattaques. Dans ce contexte, les élus sont préoccupés par l'étendue des menaces actuelles et souhaitent renforcer la sécurité informatique de la collectivité.

Dans un premier temps, la directrice générale des services (D.G.S.) vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur les cyberattaques.

10 points

Dans un deuxième temps, elle vous demande d'établir un ensemble de propositions opérationnelles visant à se prémunir de celles-ci.

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances

10 points

1) Présentation du sujet

Présenter en quelques points et une quinzaine de lignes, à l'attention des présidents de jury qui feront le choix final des sujets ainsi que des futurs correcteurs, **l'intérêt et les caractéristiques** du sujet proposé : actualité du sujet, pertinence du point de vue du grade, de la spécialité, et de la nature de l'épreuve, difficultés éventuelles du sujet, ce que ce sujet permet globalement d'évaluer chez le candidat, type de connaissances et de savoir-faire professionnels auxquels le sujet fait appel…

Les auteurs de sujet sont invités à se référer à la « note de cadrage » nationale qui présente les objectifs généraux et les attendus de l'épreuve

La cybercriminalité est un sujet d'actualités depuis plusieurs années, et l'ensemble des collectivités y sont encore aujourd'hui confrontées.

Ce sujet demande à la fois des connaissances techniques, mais également organisationnelles et managériales.

Ce sujet permettra d'évaluer l'esprit de synthèse du candidat (ne pas se perdre dans la technique qui n'est pas ici le cœur du sujet).

2) Analyse de la mise en situation et du dossier

Préciser la nature des informations fournies par la mise en situation et présenter les choix effectués en matière de composition du dossier (nature des documents, les différents angles sous lesquels le sujet est traité, les angles qui volontairement ne pas sont pas abordés dans le dossier) …

Il s'agit de présenter pour chaque document qui compose le dossier les informations centrales qu'il contient et qu'un (bon) candidat devra restituer (liste non exhaustive).

Les documents choisis apportent des réponses à des choix organisationnels, matériels ou logiciels.
Des cas concrets, et un volet juridique sont également présents.
Le piège pour les candidats, sera de ne pas se cantonner à la technique alors que les parties sensibilisation et organisationnelles (RSSI) sont les plus importantes.

Document 1 : Comment lutter contre les cyberattaques ? - Zuzana - *logpoint.com* - novembre 2020 - 4 pages.

Définition de cyberattaques ;
Conseils de protection (sauvegarde des données, contrôle accès, authentification multifacteur, sensibilisation, maj des systèmes, pare-feu/Antivirus).

Document 2 : Cyberattaques : comment se prémunir du pire - Olivier Devillers - *mairesdefrance.com* - septembre 2021 - 3 pages.

Toutes les collectivités sont des cibles potentielles des cyber-attaques
Ex. d'attaques : fraude à l'identité / cryptovirus ;

Causes / solutions : failles systèmes => maj applis / droits admin restreints / MDP ++ / sauvegardes délocalisées / se faire aider (France relance / RSSI mutualisés / audits …).

Code couleurs
Sujet / Cellule pédagogique Nationale / Concepteur sujet.

Document 3 : Comment se prémunir d'une cyberattaque ? - g*ouvernement.fr* - mars 2022 - 2 pages.

Extrait d'une communication du gouvernement sur les cyberattaques => bonnes pratiques.

Document 4 : Cybersécurité : les collectivités qui montrent l'exemple - *weka.fr* - juin 2021 - 2 pages.

Exemples d'actions mises en place dans des collectivités.

Document 5 : Les régions, soutenues par l'Anssi, déploient des centres régionaux de réponse aux incidents cyber - *francenum.gouv.fr* - juin 2022 - 1 page.

Création de centres régionaux de réponses aux incidents cyber => soutien de proximité (réponse concrète et immédiate aux victimes).

Document 6 : Former et sensibiliser les agents à la sécurité informatique pour réduire les risques - Pierre Alexandre Conte - *lagazettedescommunes.com* - septembre 2016 - 2 pages.

Sensibilisation ;
Sécurisation des lieux ;
Trier ce qu'il faut sécuriser / importance ;
Nécessité d'un suivi continu de la sécurité.

Document 7 : Cyberattaque au Département de Seine-et-Marne : Le point sur la situation - *seine-et-marne.fr* - novembre 2022 - 3 pages.

Solutions : ANSSI => RGS (cadre réglementaire) ;
Sensibilisation ;
Mutualisation des RSSI ;
Sauvegarde délocalisée ;
PCA/PRA.

Document 8 : Cyberattaques dans les hôpitaux : « Le paiement de rançon n'est pas une solution, sinon, ça devient le Far West » - Julien Lemaignen et Manon Romain - *leMonde.fr* - décembre 2022 - 3 pages.

Causes + récits de cyberattaques.

Document 9 : Pour sécuriser les petites communes, faut-il mutualiser les RSSI ? - Louis Adam - *zdnet.fr* - juin 2021 - 2 pages.

Mutualisation des RSSI pour les petites communes.

Document 10 : Cybercriminalité : « Nous ne voulons plus qu'un élu nous dise qu'il ne savait pas » - Hélène Lerivrain - *lagazettedescommunes.com* - décembre 2021 - 2 pages.

Rôle d'un RSSI : règles de sécu / analyse des risques / audit / Sensibilisation (users + élus).

Document 11 : Cyberattaques : la négligence des collectivités pourrait leur coûter cher - Lucas Boncourt - *banquedesterritoires.fr* - juillet 2022 - 2 pages.

Risques cyberattaques : préjudices financiers / perte de confiance / mise en danger d'autrui (ex des feux de circulation) / RGPD (fuite de données) $$$.

Code couleurs
Sujet / Cellule pédagogique Nationale / Concepteur sujet.

<u>Rappel du cadrage</u> : L'exploitation du dossier et les connaissances du candidat doivent lui permettre de repérer dans le dossier les informations qui lui permettront de présenter des propositions réellement opérationnelles. Il devra également dépasser les informations du dossier pour dégager des propositions réalistes, adaptées au contexte, en précisant le cas échéant les conditions et les moyens de leur réalisation : mode de gestion du projet, étapes du projet, moyens à mobiliser, contraintes… Le caractère technique de ce rapport rend pertinente, en tant que de besoin, l'élaboration de schémas, tableaux, graphiques, esquisses…

3) <u>Proposition de plan détaillé</u>

Il n'est pas attendu un corrigé type, mais une présentation sous forme d'un plan détaillé des idées centrales que l'auteur du sujet s'attend à trouver dans les (bonnes) copies. L'auteur peut donner des précisions sur le degré d'importance à ses yeux de chacune des idées listées : aspect essentiel, dont l'absence dans la copie devra être pénalisée – aspect important mais plus secondaire, dont la présence pourra être valorisée, …

***Avertissement :** il s'agit d'une proposition de plan, et non d'un plan type.*

En-tête

Comme indiqué dans la note de cadrage de l'épreuve, il est attendu une présentation du rapport sous la forme suivante :

Collectivité de …

RAPPORT TECHNIQUE
à l'attention de (destinataire)…
Objet : …..

Références (mention facultative) : celles des principaux textes juridiques ou officiels fondant le cas échéant le rapport

Introduction

*<u>Rappel du cadrage</u> : Le rapport avec propositions doit comporter **une unique introduction** d'une vingtaine de lignes rappelant le contexte et comprenant impérativement **l'annonce de chacune des deux parties** (partie informative / partie propositions). Les candidats doivent veiller à ce que l'annonce du plan aille au-delà d'une simple annonce de la structure de la copie et porte sur le contenu précis de chacune des parties.*

Plan détaillé

Rappel du cadrage : Les deux parties sont organisées en sous-parties.
Le plan est impérativement matérialisé par des titres comportant des numérotations en début des parties et sous-parties. Une transition est attendue entre la première et la deuxième partie.

I. Rapport technique sur les Cyberattaques

A. Les menaces

Qu'est-ce qu'une cyberattaque ?

Une cyberattaque désigne toute action entreprise par des cybercriminels avec à l'esprit des objectifs malveillants. Les cybercriminels lancent leurs attaques en utilisant un ou plusieurs ordinateurs afin de frapper d'autres ordinateurs, réseaux ou systèmes d'information.

Diverses méthodes peuvent être utilisées pour lancer une cyberattaque, mais les objectifs sont généralement de :

- Voler des données.
- Détruire des informations ou des données.
- Modifier des données.
- Désactiver des ordinateurs.
- Obtenir un gain financier.
- Espionner.

Exemples d'attaques

- Fraude à l'identité
- Rançongiciels
- Exploitation de failles de sécurité

Risques

- Préjudices financiers
- Perte de confiance
- Mise en danger d'autrui (ex des feux de circulation)
- RGPD (fuite de données) $$$

B. Comment s'en prémunir ?

Technique

- Sauvegarde des données, contrôle accès, authentification multifacteurs, maj des systèmes, pare-feu/Antivirus, maj applis / droits admin restreints / MDP ++ / sauvegardes délocalisées ;
- Sécurisation des lieux ;
- Trier ce qu'il faut sécuriser / importance ;
- Nécessité d'un suivi continu de la sécurité ;
- PCA/PRA.

Institutionnel

A travers son référentiel général de sécurité (RGS), l'ANSI a fixé un cadre réglementaire « permettant d'instaurer la confiance dans les échanges au sein de l'administration et avec les citoyens ».

Organisationnel

- Sensibilisation ;
- RSSI mutualisé ;
- Audits de sécurité réguliers.

Rappel du cadrage : L'exploitation du dossier et les connaissances du candidat doivent lui permettre de repérer dans le dossier les informations qui lui permettront de présenter des propositions réellement opérationnelles. Il devra également dépasser les informations du dossier pour dégager des propositions réalistes, adaptées au contexte, en précisant le cas échéant les conditions et les moyens de leur réalisation : mode de gestion du projet, étapes du projet, moyens à mobiliser, contraintes… Le caractère technique de ce rapport rend pertinente, en tant que de besoin, l'élaboration de schémas, tableaux, graphiques, esquisses

II. Propositions opérationnelles pour se prémunir des cyberattaques

- S'organiser en interne : création d'une cellule « sécurité » au sein de la DSI pouvant se réunir hebdomadairement afin de planifier des actions et évaluer les actions réalisées – Rssi mutualisé ?
- Demande d'aide financière par France Relance ;
- Evaluation de la maturité de la sécurité (via audit de sécurité ou dispositifs de l'état) ;
- Sensibiliser régulièrement l'ensemble des agents (envoi de mails de bonnes pratiques, utilisation de l'intranet …) ;
- Trier ce qu'il faut sécuriser / importance ;
- Evaluer et demander aux élus le budget nécessaire à la partie technique : Sauvegarde des données, contrôle accès, authentification multifacteurs, pare-feu/Antivirus ;
- Maj des applis ;
- Droits admins restreints ;
- Renforcer la sécurité des mots de passe ;
- Sauvegardes délocalisées ;
- Ecriture d'un PRA/PCA.

Conclusion

Rappel du cadrage : la conclusion est facultative. Elle peut toutefois utilement souligner l'essentiel, sans jamais valoriser les informations oubliées dans le développement.

Éléments pouvant être abordés dans la conclusion : (facultatif)