CONCOURS D'INGÉNIEUR 2023

EXTERNE

SPÉCIALITÉ « INGÉNIERIE, INFORMATIQUE ET SYSTÈMES D'INFORMATION »

OPTION : RÉSEAUX ET TÉLÉCOMMUNICATIONS

ÉPREUVE DE PROJET

NOTE OBTENUE : 15.25 / 20

Question 1 (a)

Ingédep Le 22/06/2023

Note à l'attention de
Monsieur le directeur des systèmes d'information

Objet : Les nouveaux enjeux en matière de cybersécurité

Les outils numériques et les données qu'il traite étant maintenant au centre de l'essentiel de nos activités professionnelles, il représente une convoitise grandissante qui expose les collectivités territoriales aux risques de cyberattaques.

Face à ces nouvelles menaces en évolutions constante, os organisations doivent s'adapter aux nouveaux enjeux en matières de cybersécruité.

Pour cela, et après un état des lieux du contexte des menaces en question et du cadre réglementaire, nous étudierons les actions préventives qu'il est possible de mettre en œuvre.

I – Cybersécurité : contexte technique et juridique

A) Le risque cybert et son évolution

Le contexte du niveau de risque en terme de cybersécurité est en pleine explosion. En 2021, une entreprise sur deux a été victime d'une attaque cyber selon les déclarations officielles mais combien l'ont également été sans s'en rendre compte.
Parmi les attaques les plus courante, on pourra noter celles par ransomware qui représente 79 % des déclarations. Leur mode d'action évolue actuellement en ajoutant au chiffrement des données et à la menace de revente une autre forme d'attaque combinée de type XXXX de service DDOS.

Ces attaques DDOS virent à bloquer le système d'information par inondation de ce dernier en masse, paralysant ainsi ce dernier qui ne peut plus répondre aux requêtes légitimes.
On compte toujours parmi l'arsenal des cybercriminels les attaques par usurpation d'identité qui virent à manipuler les agents dans un but de mal de données.
Cependant, en plus de ces types d'attaques usuelles, nous devons faire face à de nouvelles menaces telles que l'exploitation des failles Zero Day qui cible les les systèmes non mis à jour régulièrement. De plus, de nouveaux outils comme les objets connectés, plus face à pirater car moins sécurisés sont maintenant la cible eux aussi des attaquants. On voit également l'arrivée de l'intelligence artificielle que les cybercriminels comment à utiliser pour perfectionner leurs actions.
Pour la collectivité, les risques sont alors l'interruption de service, le coût financier engendré mais aussi une altération de sa réputation auprès de ses partenaires et usagés. Le risque juridique est aussi important.

B) Le cadre règlementaire :

Le risque sur les données étant au centre des menaces l'Europe a mis en place le Data Governance Act (DGA) suivi du Data Act (DA) afin de définir une stratégie de protection des données personnelles au niveau européen. Ce DGA et le DA ont également pour objectif d'attendre la souveraineté pour les données à l'horizon de 2030.
Les DGA fixe un encadrement technique et juridique des données et instaure une certification obligatoire pour les fournisseurs de données. Le Data Act complete le DGA en y intégrant les nouveaux usages des objets connectés et le Cloud Computing tout en favorisant l'interopérabilité et le renfort de protection sur l'usage illicite des données.
Toujours au niveau Européen, le règlement général sur la protection des données (RGPD) créé en 2016, aura en charge de vérifier la cohérence du DGA et du DA avec le droit des XXXX de la donnée. Le RGPD aura donc un contrôle sur le DGA et la DA.
En France, la CNIL est en charge de l'application de cela en lien avec le Comité Européen de protection des données ou EDPB.
Sur un registre plus technique, la France s'est dotée d'un outil visant à orienter et garantir un bon niveau de sécurité au organisation via le RGS ou Registre Général de Sécurité » qui est complémentaire aux recommandations de l'ANSSI.

II – Les contres mesures préventives possibles :

A) Mise en conformité et XXXX

Afin de se prévenir des risques juridiques induit par une cyberattaque, il est nécessaire de se mettre en conformité avec les exigences eu RGPD. Ces tâches seront à confier au délégué à la protection des données (DPO) et consisteront essentiellement dans la constitution d'un registre servant à recenser l'intégralité des traitements de données de la collectivité. Chaque traitement devra correspondre à une fiche contenant les informations de la donnée tel qu'un nom, un objectif, la durée de conservation et la sécurité qui y est appliquée.
Suivront ensuite des actions correctives visant à appliquer les principes de pertinence et de minimisation. Une vérification des droit d'accès des droits d'accès et de la sécurité de la donnée sera également nécessaire ainsi que la vérification du respect des délais de conservation. Enfin, le DPO devra s'assurer du respect des droits d'accès et de rectification et mettre en place des outils d'information aux usagés pour l'exercice de leurs droits.
En parallèle, des actions de formations et de sensibilisation aux risques cyber seront à mener avec la DRH afin que la sécurité du système d'information soit intégrée par l'ensembles des agents. En effet, selon une étude, 60 % des agents publics estiment avoir besoin de formation dans le numérique. De par leur manque de sensibilisation, ils représentent donc un risque pour la sécurité du système d'information.
Pour accompagner l'usage du numérique par les agents dans le cadre professionnel, une charte informatique définissant les droits et les règles devra être mise en place. Elle devra intégrer également la gestion des usages de smartphone et de périphériques USB.

B) Renforcer les moyens de protection :

En plus d'un bilan des menaces et des moyens de protection dont notre collectivité dispose actuellement, des actions préventives plus techniques peuvent être mise en œuvre. Leur objectif

étant de prévenir des trois grands risques liés à la cybersécurité : l'accès illégitime, la modification non désirée et la disparition ou vol des données.
A savoir que si un cas de vol des données se présentait, il constituerait une violation au nom de la CNIL et le DPO disposerait de 72H pour le déclarer sous peine de sanction pouvant aller à 5 ans de prison et 300000€ d'amande.
Les actions préventives auront comme objectif de renforcer la politique de mot de passe via un renouvellement périodique et une complexité XXX par exemple. La gestion du cycle de vie des comptes d'accès en lien avec la DRH ainsi que la revue régulière des droits d'accès des agents est également à mener.
Par ailleurs, une vérification des accès sécurisés aux bâtiments départementaux devra être conduite avec la direction du bâtiment.
Coté poste de travail, la vérification et l'application des mises à jour de sécurité devront être opérées ainsi que la bonne installation de l'antivirus et le verrouillage automatique des serveurs.
Enfin, la politique de gestion de sauvegarde devra être renforcée par le contrôle quotidien de ces dernières e la planification de textes de restauration.
Toutes ces mesures préventives qui ne sollicite qu'un investissement en temps sans impact financier permettront à Ingedep de renforcer son niveau de sécurité informatique.

Question 1 (b)

Afin de continuer à faire évaluer un niveau de résilience face aux cyberattaques, Ingédep doit commencer par faire un état des lieux de son niveau de protection et définir la feuille de route à suivre.

Pour cela, un audit du système d'information devra être commandé auprès d'un cabinet d'expertise spécialisé dans ce domaine.
Avant de lancer le marché pour la commande de cette prestation, nous devrons nous rapprocher des services de l'Etat tel que l'ANSSI afin d'étudier les possibilités d'accompagnement dans ce domaine. De plus l'Etat ayant débloqué un budget de 1,7 milliard d'euros dans le cadre du plan France Relance visent à accompagner les collectivités dans leur transformation numérique, il sera alors intéressant d'étudier avec l'ANSSI les possibilités de subvention de l'audit mais également des actions qui en découleront.

A noter que l'ANSSI dispose maintenant de centres régionaux nommés CSIRT pour Computer Secruity Incident Response Team qui ont pour mission la sensibilisation ainsi que la communication des alertes de sécurité. Ces CSIRT ont également un rôle de postage des retours d'expérience et il serait donc intéressant de les intégrer à notre démarche.
Pour revenir à l'audit, il devra se concentrer principalement sur trois axes et, pour chacun de ces axes, il devra prévoir une analyse de l'existant à Ingédep puis une évaluation de cet existant par rapport aux exigences et aux standards actuels. Enfin, et sur chacun de ces axes, l'audit devra définir une feuille de route chiffrée et prioriser sur les actions correctives que nous devrons mettre en œuvre. La priorisation des actions sera à définir en collaboration avec la Direction d'Ingedep.
Les axes à étudier seront alors :

- Réglementaire : tel que la conformité au RGPD
- Sécurité externe : analyse et test de niveau de sécurité de nos services externalisés tels que site internet, application XXX et cloud
- Sécurité interne : analyse et test de niveau de sécurité de nos infrastructures réseaux et serveurs.

Le rapport d'audit attendu de la société retenue devra intégrer à minima l'ensemble de ces points et, si besoin, prévenir des tests réels de sécurité tel qu'une simulation d'attaque externe, interne ou l'envoi d'un faux mail de phishing aux agents.
Enfin, le rapport d'audit devra prévoir des indicateurs de suivi et une seconde phase d'évaluation après mise en œuvre des actions correctives qui auront été validées par Ingedep.

Question 2

Les risques en matière de cybersécurité ainsi que les types de menaces évoluent en permanence et très rapidement. L'arrivée de l'intelligence artificielle va très certainement encore accélérer ce phénomène dans les mois à venir.

Pour entrer ces nouvelles menaces, les outils de sécurité tel que firewall et antivirus doivent eux aussi évaluer et s'adapter. En tant que collectivité ayant en charge la sécurisation de 4800 postes de travail, Ingedep doit également prendre en considération ces évaluations.

1 – Les firewalls de nouvelle génération :
Ces nouveaux modèles, en plus des fonctionnalités traditionnelles de filtrage réseau et de protocole, renforcent leur niveau d'inspection des paquets réseaux qu'ils analysent via les sondes IPS. En plus de la conformité au RFC, les mécanismes IPS sont désormais en mesure de différencier les applications légitimes des applications non autorisées via leur signature numérique.

Ainsi, les firewalls de nouvelle génération vont mieux arriver face à la détection des logiciels malveillants et ont une spectre d'action plus large que leur prédécesseur grace eux aussi à une optimisation par l'intelligence artificielle.
Ils offrent également l'analyse des trames chiffrées via HTTPS afin de détecter toute attaque exploitant cette faiblesse des anciennes générations de firewall.
Enfin, ils vont désormais équiper pour l'analyse et la sécurisation des échanges avec le Cloud tel que les applications en SaaS ou les connection VPN ou Zero Trust ZTNA.

2 - Les nouveaux antivirus :
Les antivirus actuels sont basés sur l'analyse de signature numérique laissée par le virus déjà connu. Ce mode de fonctionnement nécessite des mises à jour régulières de l'ensemble des postes de travail et diminue leur performance. Ces derniers sont donc consommateur de ressources et vont en plus inefficace face aux nouvelles menaces Zero Day qui, par définition, n'ont pas de navigateur connu.

Les nouveaux antivirus sont intelligences artificielles. On notera deux types de nouveaux antivius que sont les EDR qui analyse le comportement d'un fichier ou d'un poste et les XDR qui rajoute une fonctionnalité de machine learning visant à mutualiser les détections sur l'ensemble des systèmes connectés. A noter que les XDR sont plus dépendant du Cloud de par leur fonctionnement.

N'étant plus basé sur des navigateurs, ces nouveaux antivirus orientés Cloud, libèrent les postes de travail en terme de performance et ne nécessite plus de mise à jour.
De plus, leur fonctionnement sur le comportement ne limite plus leur action sur les fichiers via signature et sont donc plus efficaces sur les nouvelles menace type Zero Day.
Enfin, de par leur fonctionnement lié au Cloud et non au poste de travail, il représente un allégement de la charge de travail des équipes informatiques via une installation rapide et l'absence de mise à jour.

Les nouveaux outils de sécurité tel que firewall et antivirus de nouvelle génération représente un réel gain en terme de sécurité. Par ailleurs, leurs temps de retour sur investissement sont assez courts. Il représente donc une bonne opportunité pour Ingédep de faire évoluer sensiblement son niveau de sécurité

Question 2

CCTP de renouvellement du firewall et de l'antivirus

1 – Objet du marché
Face aux nouvelles menaces et au nouveaux risque en matière de cybersécurité, le présent marché à pour objet le renouvellement des solutions firewall et antivirus actuellement en production au sein d'Ingedep.
Les candidats devront détailler dans leur offre les mesures et la méthodologie qui sera mise en œuvre pour éviter toute coupure de service durant les opérations de bascule entre la solution actuelle et la solution préparée.

2 – Contexte
Le département d'Ingédep est divisé en 75 sites géographiques interconnectés dont 40 collèges qui ont des contraintes spécifiques de sécurité lié à la réparation des réseaux administratifs et pédagogiques en lien avec le rectorat. L'ensemble des sites sont, selon leur éloignement, soit au siège d'Ingédep via des fibres noires, soit par des liens opérateurs via des VPN. De plus, plusieurs VLAN sont en production et sont susceptibles d'être interconnectés entre plusieurs sites.
Ingédep est également équipé de près de 4200 postes informatiques ainsi que de tablette tactile. Sur ce poste, environ 1800 poste sont rattachés au réseau des agents du département.

3 – Prestations attendues :
A) Firewall
Le département dispose actuellement d'un firewall qu'il souhaite remplacer par un modèle de nouvelle génération.
Les fonctionnalités attendues sont :
- Gestion multi-réseau et multi-VLAN
- Filtrage protocolaire
- NAT et PAT
- Déchiffrage SSL et ronde IPS
- Centralisateur VPN avec ouverture VERS LE ZTNA
- Mode IPS avancé avec identification des applications
- Filtrage par application et détection de malware
- Filtrage via géolocalisation des IP sources et destination
- Gestion avancée des droits d'administration
- Edition de rapport (correction, alerte….)
- Analyse avancé des log
- Comptabilité avec les plaformes SOC

B) Antivirus
Ingedep dispose actuellement d'un antivirus basé sur l'analyse de signature. Les candidats devront préparer dans leur offre son remplacement par un antivirus de nouvelle génération répondant à minima aux fonctionnalités suivantes :
- Client léger n'impactant pas la performance des postes de travail.
- Un fonctionnement « off-line » du moteur de l'antivirus afin d'être efficace même sans connexion.
- Une protection avancée contre les riques Zero Day.
- Une Plate-forme de gestion centralisée permettant d'avoir une vision d'ensemble des postes et servers protégé par la solution.
- Gestion avancé des droits d'administration.
- Edition de rapport.
- Comptabilité avec les plateformes SOC

4 – Maintenance :
Les offres devront intégrer la maintenance corrective et évolutive de la solution pour la durée du marché avec une GTR de 2h sur les incidents critiques.

Question 3

Ingédep 22/06/2023

Note à l'attention de

Monsieur le Directeur des systèmes d'information

Objet : Le cloud computing

Depuis la crise sanitaire liée au Covid 19, la numérisation des services publics a subi une accélération afin de pouvoir garantir un accès aux français. Le cloud computing a alors permis cette monté en charge et l'Etat a ainsi défini sa nouvelle stratégie numérique : « Cloud au centre ». Face à cette mutation des services numériques, Ingédep doit également analyser les opportunités du cloud computing.

Ainsi, après avoir analysé les bénéfices et les opportunités de ce nouvel outil, nous en étudierons les faiblesses et les points de vigilance.

I – Les possibilités offertes par le cloud :

A) Les bénéfices

L'avantage principal du cloud est en faculté de monté en charge rapide avec un accès instantané à de nouvelles ressources ou infrastructures.

Les organisations peuvent ainsi rapidement mettre en œuvre de nouveaux services sans être dépendant des livraisons de nouveaux équipements serveurs ou réseaux. L'accès à de nouvelles plateformes serveurs étant alors rendu instantané et l'usage y étant facturé à la consommation. Ce modèle économique à l'avantage de ne coûter que ce que l'on consomme pour immobilisation du matériel souvent sous-exploité.

De part en nature, le cloud favorise également la mise en place de nouveaux services publiés à la population mais également à destination des agents. Ainsi, avec le développement du télétravail, le cloud offre la facilité de mettre en place de nouveaux outils collaboratifs tels que la visioconférence, la messagerie ou les espaces de partage de fichiers.

De part, la redondance des équipements coté hébergeur des solutions Cloud, ce dernier apporte également une augmentation de la résilience des services et participe ainsi à la confiance des français dans la fiabilité de leurs services publics.

B) Opportunités

Pour les collectivités territoriales, l'opportunité du Cloud est alors la possibilité de développer rapidement une nouvelle opération de services publics numériques. Il représente donc un outil essentiel de l'accélération de la transformation numérique des collectivités impulsées par les directives de l'Etat ?
Ainsi, le Cloud simplifie la dématérialisation des procédures et des démarches

administratives des français en permettant aux organisations une réactivité accrue par rapport aux solutions physiques d'hébergement.

Le Cloud est également moteur dans la digitalisation des usages internes des agents via de nouveau outil de collaborations et d'échanges dont le besoin accompagne le télétravail.

II – Les limitations du Cloud :

A) Les faiblesses :

Malheureusement, tout n'est pas absolument parfait avec le Cloud qui, de par l'externalisation des infrastructures engendre de nouvelles faiblesses des systèmes d'information.

En effet, l'essentiel des activités Cloud XXX par le revenu et principalement la connexion internet de la collectivité.

En cas de sous dimensionnement du lien, de XX tolérance à la XXX, les accès aux outils Cloud peuvent alors être dégradés voir interrompus.

Des risques nouveaux de sécurité peuvent aussi être notés dans le XXX ou une partie de la sécurité des infrastructures reste opaque et fermée à la vue du client qui doit faire confiance à l'hébergeur.

De plus, les solutions Cloud étant accessibles via connexion internet, la surface d'attaque et donc le risque de cyberattaque augmente. Les utilisateurs devront alors être sensibilisés aux risques liés à ces nouveaux outils et la DSI devra imposer une politique de gestion des notes de XXXX adpatée.

B) Points de vigilance :

Au niveau des équipes de la DSI, il sera nécessaire de prévoir des formations spécifiques aux outils d'administration liés au Cloud et de suivre ces évolutions par de la vieille technologie et des servions de remise à niveau. Des aides de la DINUM sont à étudier pour le financement de ces formations.

De plus, les CCTP lié à l'acquisition ou à l'utilisation d'infrastructure Cloud ou de solution logiciel type XXXX devront intégrer des exigences quant aux niveaux de disponibilité du service et de la sécurité mise en œuvre par l'hébergeur. Une clause d'auditabilité pourra également être intégrée aux marchés. Par ailleurs, les CCPT devront XXXX que l'hébergeur soit certifié SecNumCloud afin de garantir le respect des règles du RGPD et assurer les bonnes règles de gestion de données sensibles.

Un point de vigilance sera également à surveiller sur le budget de la DSI, les solutions Cloud, de par leur facilités d'accès et leur fonctionnement peuvent induire des augmentations sensibles des lignes de crédit.

Les solutions Cloud sont de très bon outils de croissance des évolutions numériques des services publics. Cependant, leur utilisation doit rester raisonnée afin de reprendre à des besoins spécifiques. L'essentiel du service étant porté par l'hébergeur, le choix de ce dernier se fera judicieusement afin d'éviter tout impact sur la continuité de service. On pourra prendre en exemple l'incendie d'OVH en 2021 qui conduit à de nombreuses pertes de données.

Question 4 (a)

Dans le cadre du projet de migration de notre suite office 2010 vers office 365, je vous propose de suivre les étapes suivantes :

1 – Audit des nuages :

L'objectif étant ici d'analyser nos usages actuels d'office 2010 afin de dimensionner au mieux notre besoin pour migrer à Office 365.

Ainsi, nous devrons obtenir ici le nombre de postes équipés de la suite 2010 et, parmi ces derniers, différencier ceux utilisés uniquement pour la bureautique et ceux utilisant également la messagerie.

Nous obtiendrons ainsi le nombre de compte de messagerie et, sur ces derniers, nous devrons en analyser les usages en terme de stockage pour chaque boite.

Toujours sur la messagerie, une extraction complète des comptes de services et des listes de diffusion sera également à faire avec une cartographie des accès de chacun.

2 – Définition du besoin global :

En fonction du nombre de compte de messagerie et de leur usage en stockage, il sera alors possible de définir le nombre et le type de licences Office 365 que nous devrons commander. En effet, en fonction des usages, il sera possible d'affecter une licence différente à chaque agent. Cette différenciation n'affectant pas leur besoin, elle permettre de limiter fortement les coûts liés aux licences.

Nous pourrons donc ensuite définir une estimation financière du projet grâce à cette volumétrie de licences à acquérir. A noter que cette dépense sera récurrente car elle correspond à une dépense annuelle de fonctionnement.

Le calcul de l'enveloppe budgétaire du projet devra également intégrer une prestation de paramétrage et de migration des données sur le budget d'investissement.

Toujours sur le besoin, il sera important de prendre en compte la délocalisation des données et des usages qui pourra avoir un impact sur le délit nécessaire de notre connexion internet.

3 – Communiquer :

Dès les premières places du projet, il sera nécessaire de prévoir un plan de communication à destination des agents mais également de la Direction générale et des Elus. Nous détaillons ce dernier par la vente.

4 – Rédaction du CCTP :

La rédaction du cahier des charges pourra alors être réaliser. Ce dernier devra prévoir les prestations de paramétrage de la plateforme Office 365, la création et la sécurisation du tenant Microsoft avec durcissement de la sécurité ainsi qu'une solution de sauvegarde spécifique à Office 365 et prenant en charge l'intégralité des données hébergées.

La prestation intégrera également l'acquisition des licences et la prestation de migration des données des utilisateurs vers le Cloud.

5 – Migration :

La migration vers Office 365 conduit par le prestataire retenu, devra suivre les étapes suivantes :

- Création du Tenant Microsoft avec paramétrage et durcissement de la sécurité
- Mise en place de mécanisme de renvoi de mail entre ancien et nouveau système de messagerie. La migration se faisant de manière progressive, cette fonctionnalité est indispensable.

La planification des migrations pourra alors commencer et suivre les étapes suivantes :

- Test 1 : Qualification
  Une première migration de l'ensemble des comptes de la DSI permettra de valider la procédure et le tester le plan de communication et d'accompagnement.
- Test 2 : Validation
  Un second test grandeur nature sera réaliser sur l'ensemble d'une direction du siège. Elle permettra de conforter les procédures avant le déploiement général.
- Migration général
  Suivant un calendrier précis et découper en plusieurs étapes, la migration sera alors réalisée de manière progressive sur l'ensemble des directions. Ce découpage permettra de mettre en place des équipes DSI XXX de rapport pour les agents afin de les accompagner dans leur transition vers Office 365.

Question 4 (b) :

Tout au long du projet, des actions de communication devront être conduites afin de préparer puis d'accompagner les agents dans cette migration.
En effet, Office 2010 et leur messagerie représentent pour la majorité de nos collègues l'outil central de leurs activités. La conduite du changement sera donc un point essentiel de la réussite de ce projet.
En premier lieu, et après les tapes de définition des besoins suites à nos inventaires, une présentation du projet devra être portée en réunion de Direction générale afin que chaque DGA et Direction prennent la mesure du changement à venir. Cette présentation sera accompagnée d'une projection powerpoint qui sera ensuite envoyée à l'ensemble des directeurs.
L'essentiel de la communication devra ensuite être orienté vers les agents. Dès la présentation en réunion de Direction, des actions de communication seront faites via l'intranet afin de les avertir du changement, de leur communiquer un calendrier général du projet et leur présenter les avantages du nouvel outil. Une plaquette de présentation et de prise en main leur sera leur sera ensuite communiquée via l'intranet, puis individuellement par mail.
En fonction du planning du projet, de nouvelles communications seront envoyées aux agents pour les tenir informer puis, quelques semaines avant la migration, des ateliers seront organisées sur chaque sites géographiques. Ces derniers permettront aux agents de participer au projet aux même.