

CONCOURS D'INGÉNIEUR 2025

INTERNE

SPÉCIALITÉ « INFORMATIQUE ET SYSTÈMES D'INFORMATION »

OPTION « RÉSEAUX ET TÉLÉCOMMUNICATION »

ÉPREUVE DE PROJET

Question 2

Conseil départemental d'Ingédep

le 19 juin 2026

Note à l'attention du
Directeur des Systèmes d'information

Objet : Préconisations techniques et organisationnelles pour la sécurisation de l'administration du système d'information d'Ingédep

Référence : Directive (UE) 2022/2555 du parlement européen et du Conseil du 14/12/22 sur les mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'UE

L'administration des systèmes informatiques est essentielle afin de maintenir notre système d'information (SI) opérationnel et à jour. L'accès distant représente un risque majeur en cas de cyberattaque ce qui pourrait compromettre la fiabilité et la confidentialité de nos données.

Face aux attaques de plus en plus présentes, l'Europe a accentué la législation en vigueur. Le conseil départemental d'Ingédep s'est saisi du sujet et souhaite connaître les préconisations en vue de la sécurisation de l'administration de son SI à distance.

Nous verrons dans une première partie la définition et les enjeux concernant la sécurisation de l'administration distante (I). Une deuxième partie traitera des leviers de mise en œuvre en évoquant la réglementation et les points de vigilances associés (II).

I- La sécurisation de l'administration du SI, en enjeu de taille pour les collectivités territoriales (CT)

A- L'administration à distance, un avantage qui peut devenir un poids

Dans un système d'information, certains comptes disposent de privilèges d'administration comme les sociétés d'infogérance, les équipes de la DSI, le RSSI ou tout autre intervenant ayant besoin d'accéder au SI pour son administration. En fonction de la localité de l'individu, la connexion peut soit se faire en interne (DSI, RSSI) ou en externe (Société extérieure, télétravailleurs). L'accès se fait généralement depuis un poste lambda ce qui représente une faille considérable au niveau du SI.

Plusieurs recommandations sont donc à prendre en compte afin de limiter la surface d'attaque en utilisant un réseau d'administration dédié physique ou logique si la difficulté de mise en œuvre est trop forte. Un filtrage de flux sera nécessaire ainsi qu'une revue des droits d'accès et leur journalisation.

B- L'impact d'une cyberattaque sur Ingédep non sans conséquences

Les enjeux d'une intrusion dans notre système d'information seraient conséquents. En effet, certains comptes de nos prestataires ou administrateurs détiennent des informations sensibles sur Ingédep, comme, par exemple, le plan des routes et de circulation du département.

Une compromission des données pourrait impacter la vie de nombreux de nos usagers. L'image du département pourrait aussi se voir incriminée. La détermination des personnes accédant au SI est donc primordiale et doit être surveillée continuellement.

Nous allons maintenant évoquer des préconisations de mise en œuvre et la réglementation associée.

II- Mis en œuvre de la sécurisation de l'administration du SI

A- Des préconisations opérationnelles pour se protéger

La recommandation de l'ANSSI relative à l'administration sécurisée du système d'information établit plusieurs recommandations importantes sur lesquelles nous pouvons nous appuyer.

La mise en place d'un réseau d'administration physique ou logique permettra de réduire la surface d'attaque. Un filtrage concernant les flux à autoriser sera nécessaire pour éviter l'escalade dans nos équipements.

Nous établirons une matrice des flux pour réguler le trafic réseau. La mise en place d'une journalisation des accès et sa centralisation seront un plus indéniable (Syslog, Graylog, ELK).

Les accès distants de nos prestataires et télétravailleurs devront passer systématiquement par un tunnel VPN IPSEC sécurisé. Un classement logique de sous-réseaux à l'aide de VLAN permettra de contenir l'infection.

Dans un second type, l'étude de la mise en place d'un bastion type Rhybat permettra d'avoir un seul point d'entrée sécurisé afin de journaliser les actions. La solution PAM (Privileged Access Management) permettrait en plus un coffre-fort des mots de passe, un audit et une meilleure visibilité ; il est également conforme ANSSI, ISO 27001 et RGPD, ce qui est un plus.

B- Une réglementation européenne pour encadrer les collectivités

L'Europe a établi, au travers de la NIS 2 (Network and Information System) et du RGPD (Registre Général sur la Protection des Données), des mesures qu'il conviendra de respecter.

Il faudra adapter la sécurité du SI au risque en établissant une politique d'analyse d'attaques, une déclaration au CSIRT dans les 24 heures à 72 heures. Nous devons établir un projet final sous un mois de l'attaque et informer nos usagers si des données sensibles les concernant ont fuitées. Suite à une cyberattaque en 2023, le CHRU de Brest a limité son impact grâce à sa réactivité et sa collaboration avec l'ANSSI.

Ces préconisations devront faire l'objet d'une révision annuelle et une veille cyber sera plus que nécessaire.

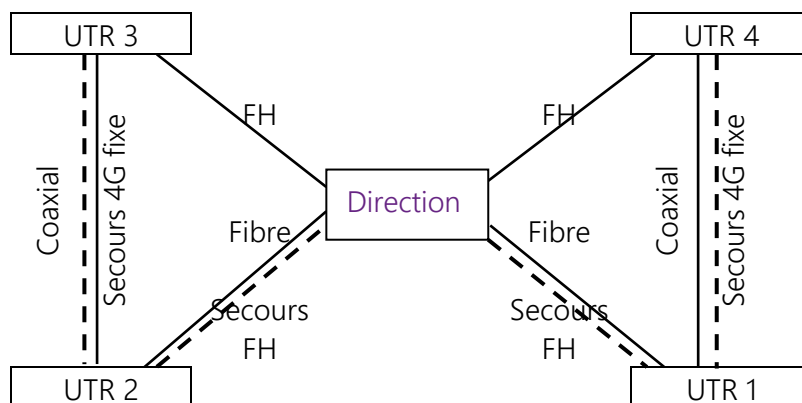
Question 1

L'architecture montagneuse du département d'Ingédep complexifie l'interconnexion des différentes unités territoriales routières (UTR) au site principal de la Direction.

La liaison actuelle ne permet pas le secours des UTR en cas de rupture du lien la reliant au site principal. Il convient donc, dans un premier temps, d'étudier la mise en place d'un lien de secours pour faire le reboutage. Voici le tableau récapitulatif des différentes technologies internet sur le marché :

Technologies	Avantages	Inconvénients
Fibre optique	Fil de verre, débits élevés, pas de perturbation, type FTTO, PITH, FITE, 100 Mbits/s à 1Gbits/s	Nécessite des travaux et une éligibilité, couverture difficile en montagne
ADSL	Déjà déployée sur tout le territoire, utilise la ligne téléphonique	Débit faible et asymétrique, technologie en cours d'arrêt.
FITTLA (Coaxial)	Bonne alternative à l'ADSL utilisé historiquement pour la TV, câblage hybride, simple et peu coûteux.	Débit asymétrique, 16 bits/s en téléchargement, 100 Mbits/s montant
4G fixe	Couverture en zone blanche, signal 4G → Wifi	Soumis à éligibilité, uniquement internet
Satellite	Bonne alternative, nécessite une parabole	140 000 k parcouru pour requête, latence élevée
FH	Pas de génie civil (GC), sans fil, peu coûteux, fournit par les opérateurs, facile à mettre en œuvre	Abonnement mensuel + frais d'accès au service, soumis aux conditions climatiques, interférence et perturbation à prévoir un surcoût en montagne

Je propose d'utiliser en lien de secours les deux FH ver UTR1 et UTR2 car encore actifs. Voici un schéma avec les évolutions possibles :



Les UTR 1 et 2 seront secourus via leur ancien lien FH en cas de rupture de la fibre jusqu'à la direction (pas de coût supplémentaire). Je propose de relier les UTR 3 et respectivement aux UTR 2 et 1 afin d'avoir une redondance filaire coaxiale et sans fil 4G fixe s'il y a une perturbation du signal radio (interférences, tempêtes...).

Dans une version évolutive, il pourrait être envisagé de relier les UTR1 et 2, et UTR3 et pour un maillage total.

Les évolutions proposées permettent l'utilisation, via Coaxial et 4G fixe, des outils informatiques et téléphoniques avec un débit revu à la baisse mais fonctionnel (mode dégradé). Une technologie URRP serait envisageable en cas de coupure du lien internet principal (actif-passif opérateur).

Après le choix de la technologie de connexion, il convient de comparer et choisir le protocole de routage le plus adapté à la situation.

Deux protocoles sortent du lot :

- EIGRP pour Enhanced Interior Gateway Routing Protoc
Son principal inconvénient est qu'il est propriétaire CISCO. Il prend en compte l'équilibrage de charge, évite les boucles, fait le routage inter-domaine et la commutation est très rapide. Cependant, sa configuration paraît complexe à mettre en œuvre et ne prend en charge que le protocole IP.
- OSPF pour open Shortest Path Fist
Développé par l'IEFT, compatible multi-constructeurs, routage efficace à l'état de lien, prise en charge des réseaux complexes et multi-fournisseurs.

EIGRP offre une convergence plus rapide que le protocole OSPF mais OSPF a l'avantage de l'équilibrage de charge et utilise plusieurs chemins vers la même destination. Je choisirais donc OSPF au vu de l'architecture ; de plus, nous n'avons pas les données matérielles afin de confirmer une architecture intégrale en marque CISCO. L'Intelligence Artificielle pourra être un appui de taille pour la gestion du bouclage, la détection d'activité et de diagnostic en contrepartie d'un apprentissage nécessaire.

Question 3

Les entreprises et collectivités sont de plus en plus la cible d'attaques cyber et phishing. En effet, la donnée est devenue le nerf de la guerre et donc un objet convoité. Afin de se mettre en conformité avec l'article 21 de la NIS2, il convient d'en étudier l'existant pour ensuite proposer des solutions techniques et opérationnelles. Une démarche projet viendra ensuite compléter ses propositions.

I- Identifier les failles et les menaces potentielles

Plusieurs menaces peuvent impacter notre SI, voici les principales :

- Phishing : consiste à envoyer des messages frauduleux en usurpant l'identité d'un tiers pour amener la personne à divulguer une information sensible (données personnelles...).
- Ransomware : bloque l'accès au SI en chiffrant et demandant une rançon.
- Deni de service (Ddos) : rendre un service inaccessible en le saturant de demandes de connexion.

Un audit du système permettra d'en analyser la surface d'attaque et son impact sur l'Ingédep. Il conviendra, comme décrit dans l'article 21 de la NIS2, de se préparer au mieux en anticipant avec ce plan d'action :

- 1- Évaluer les besoins de sécurité et les acteurs critiques.
- 2- Sélectionner les outils de sécurité les plus adaptés au SI.
- 3- Recruter et former du personnel qualifié en cybersécurité.
- 4- Formaliser des procédures opérationnelles pour être prêt en cas d'attaque.
- 5- Évaluer en continu les lacunes du SI.
- 6- Sécuriser l'accès aux locaux et la gestion des actifs RH.
- 7- Activation authentification multi-facteurs (MFA).

Toutes ces actions nous amènent au choix d'un système de sécurité.

II- L'équipement de sécurité, un atout pour atténuer une cyberattaque

Plusieurs technologies avec des fonctionnalités différentes ou complémentaires intégrant l'IA existent sur le marché.

Le SOC (Security Operation Center) est une plateforme centralisée garantissant la sécurité de l'entreprise. Il permet d'identifier les menaces avec différents protocoles (surveillance permanente, activité suspecte, analyse comportementale), détecte les intrusions et permet une réponse active aux menaces avec des mesures immédiates. Il fonctionne en continu 24h/24. Le choix se portera sur l'interne qui implique des ressources disponibles et formées, ou externe géré par un prestataire spécialisé.

Les antivirus EDR (Endpoint detection response) protègent les terminaux comme les ordinateurs, tablettes... en collectant les données. Il pourrait être couplé à un XDR pour inclure l'intégralité du réseau pour permettre une réponse rapide. L'XDR analyse différentes sources de données.

III- Mise en place d'un PRI / PCI

Le Plan de Reprise Informatique (PRI) est un manuel d'urgence qui définit les objectifs de reprise pour minimiser le temps d'arrêt. Il cartographie les actifs, permet la mise en place des procédures de sauvegarde et restauration, et clarifie les responsabilités en cas d'incident.

Le Plan de Continuité Informatique (PCI) se concentre sur la prévention et l'anticipation en garantissant la continuité de fonctionnement. Il permet d'analyser les risques, de mettre en place

une redondance du système, un plan de sauvegarde et de former le personnel pour répondre aux incidents.

Après avoir vu les différentes étapes pour assurer une détection et une réponse aux incidents, nous allons détailler la démarche projet associée.

IV- Démarche projet à mettre en œuvre

A- Cadrage du projet

Il faudra commencer par vérifier la faisabilité du projet avec un premier diagnostic. Les questions budgétaires, humaines et juridiques seront évoquées ainsi qu'une recherche de financement.

B- Planification

La planification avec un diagramme de GANTT permettra une vision globale des ressources nécessaires au projet. La gouvernance sera ensuite mise en place avec deux comités :

- COPIL (Comité de pilotage) : arbitrage du projet, regroupe 5 à 8 personnes décideuses telles qu'élu, DGS, DGA, DSI, financiers. Il se réunira tous les trimestres.
- COTECH (Comité technique) : vérifie la faisabilité et la validation technique, regroupe une dizaine de spécialistes tels que la DSIN, RH, finances, marchés, prestataires. Il se réunira une fois par mois.

C- Conception / réalisation

Achat de matériel, choix des technologies et paramétrage.

Choix du financement : suivant les modalités d'acquisition, les boîtiers seront achetés sur le budget d'investissement et les abonnements annuels sur les licences seront pris sur le budget fonctionnement.

Le projet devra être intégré au Débat d'Orientation Budgétaire (DOB) pour être intégré au Budget Primitif (BP) avant le 31 mars. Des Décisions Modificatives (DM) pourraient ajuster le budget au besoin en cours d'années. Il pourra être étudié un Plan Pluriannuel d'Investissement (PPI) sur plusieurs années. Un marché public sera réalisé pour intégrer au cahier des charges les clauses techniques et particulières (CCTP), les bordereaux des prix unitaires (BPU), CCAP. Toutes ces pièces ainsi que l'acte d'engagement seront intégrés au dossier de consultation des entreprises (BCE). Les contraintes organisationnelles y seront décrites (HNO, sans coupure). Il pourra être envisagé un déploiement pilote avant sa généralisation.

D- Accompagnement / Bilan

Un plan de formation et de communication sera établi pour informer les agents et les élus des nouvelles sécurités mises en place et leur impact sur leurs activités quotidiennes. La communication pourra se faire suivant les besoins en réunion d'information, vidéos, mail, site internet et affiches internes. Elle aura lieu en amont pour présenter les changements, pendant et après, pour recueillir les retours éventuels des utilisateurs. Un retour d'expérience (RETEX) ainsi qu'un sondage destiné à recueillir les blocages éventuels pourra être mis en place.

Question 4

L'article 20 de la directive NIS2 oblige les organes de direction à se former sur les risques liés à une attaque informatique pour en évaluer les impacts. Cette directive incluant aussi les usagers et personnels du conseil départemental, ils seront également intégrés à cette démarche. Nous proposerons, dans une première partie, des actions à destination de la direction et des élus d'Ingédep (I). Une seconde partie ciblera les agents et les usagers (II).

I- Former les élus et la direction pour mieux se protéger

L'anticipation et la formation permettent de faire baisser la criticité des attaques informatiques à condition de bien être impliqués et conscients.

La DSIN pourra organiser des sessions de formation et de sensibilisation lors des COPIL pour y intégrer direction, chefs de services ainsi que les élus. Ingédep pourra faire appel à un cabinet externe spécialisé pour avoir plus d'impact et de répercussions. Orange Cyberdefense a ouvert un campus dans le sud de la France, à Marseille, et aide les entreprises à se protéger. Le campus est assez discret mais regroupe 105 experts cyber (hacker éthiques, analystes...) sur 1 100 m².

Trois domaines d'activités sont couverts :

- La prévention : permet d'explorer les vulnérabilités en simulant une attaque pour mesurer ensuite notre réactivité
- La détection : pour cerner la menace et la bloquer
- La protection : avec un accompagnement personnel des clients.

II- Les agents et les usagers : une cible de choix pour les cyberattaques

Les agents du département sont une cible privilégiée des hackers de part leur contact quotidien avec différents prestataires. La sécurisation du Système d'Information d'Ingédep passe donc naturellement par la sensibilisation de ses agents. Orange Cyberdefense propose des tests réels d'intrusion comme le piratage des badges d'accès, la récupération des mots de passe via la messagerie ou encore le changement des prix d'un site internet. Un tel test grandeur réelle permettrait d'analyser le niveau de conscience de nos agents et leur vulnérabilité.

La DSIN se propose de faire des réunions de sensibilisation ainsi que des webinaires sur le sujet une fois par mois pour commencer.

Un plan de communication à destination de nos usagers via le site internet du département ou article de presse permettra de leur faire comprendre l'impact d'une telle attaque sur le département mais également dans leur vie privée et professionnelle.