2

CYBERSECURITE

ANNEXES

RAPPORT SUR LE DEVELOPPEMENT DES USAGES

COMPTE RENDU D'AUDITION

I] Groupe de travail : Cybersécurité

Date de l'entretien : 29/04/2022

Agents présents : Julie LELEU, Pierre KREMER

Nom de la collectivité ou de l'organisme : Syndicat Mixte COGITIS

Personne contactée : M. VEROLLET

Fonction dans la structure : Chef de service gestion infrastructure et responsable informatique

Tel : 04 67 16 18 00 / 06 31 07 37 10

Mail : tverollet@cogitis.fr

Site internet : cogitis.fr

Remarques :

Transfert obligatoire pour les personnes morales de la compétence « veille technologique et réglementaire liées aux évolutions dans le domaine des technologies de l'information et de la communication »
2 pôles de clients : les Départements et les Communes (+CC)
Soit adhérent qui bénéficie des services proposés
Soit client qui bénéficient de prestations de services

II] Avant l'audition

Singularité du projet : Assure et propose des solutions sur 10 missions statutaires :

- **Veille technologique et réglementaire (compétence obligatoire)**
- Études préalables à la réalisation de projets informatiques
- Conseil aux maîtres d'ouvrages dans le choix de solutions et maîtrise d'œuvre d'opérations techniques
- Installation de solutions logicielles et intégration à l'architecture informatique existante
- Développement et / ou maintenance de solutions logicielles spécifiques
- Gestion opérationnelle des infrastructures techniques
- Gestion technique de la téléphonie et de la visiophonie
- Assistance utilisateurs et / ou exploitation des solutions mises en œuvre
- Formation des agents à l'utilisation de logiciels métiers ou bureautiques
- Délivrance de services d'administration numérique

RAPPORT SUR LE DEVELOPPEMENT DES USAGES

COMPTE RENDU D'AUDITION

III] Présentation de la collectivité

Statut juridique : SPIC (Essaimage)

Date de création : créé par arrêté préfectoral le 15/01/1998

Périmètre d'action / membre : CD Hérault, Aude et Jura / CDG Hérault / SDIS Hérault et Jura / EIDLM

Nombre d'agents : 130 salariés, soumis au droit privé sauf Comptable et Directeur

Fonctionnement de la collectivité : Comité de 13 représentants parmi les membres et bureau avec 4 membres (président / 2 vice-présidents / un secrétaire)

IV] Présentation du projet

Contexte politique de la mise en œuvre : volonté des départements de répondre à un besoin de mutualisation dans le domaine du numérique, accompagnement des communes et EPCI dans la transformation numérique

Description :

Schéma / structure juridique :
Syndicat Mixte Informatique, avec transfert obligatoire pour les personnes morales de la compétence « veille technologique et réglementaire liées aux évolutions dans le domaine des technologies de l'information et de la communication »
Existence de 2 pôles de clients : soit les adhérents qui bénéficient des services proposés, soit les clients, qui bénéficient de prestations de service.
Pour information, COGITIS comporte 28 adhérents (Conseils Départementaux, établissements publics, communes et EPCI)

Quatre blocs sont proposés :

- Infogérance et assistance informatique
- Conseil et expertise
- Formation
- Services numériques

Cout du projet : COGITIS a un budget d'environ 10M€/an

Financement : le financement passe par la facturation des services, au prix coûtant. Il n'y a pas de frais d'adhésion. Pour information, une prestation de conseil/expertise est facturée en moyenne entre 600€ - 1000€ la journée.

Nombre d'agents en charge du projet et répartition par filière et grade : 130 agents

Durée de lancement / initiation du projet : COGITIS a été créé en 1998 et a donc plus de 24 ans d'existence.

RAPPORT SUR LE DEVELOPPEMENT DES USAGES

COMPTE RENDU D'AUDITION

Evolutions envisagées :

- Acquisition de logiciels métier
- Groupements d'achat (mais très peu plébiscités par les membres)
- Archivage numérique
- Fourniture de certificats électroniques
- Observatoire de l'informatique des communes
- Veille réglementaire et mise en conformité pour ses membres
- Informatique des écoles

Mission et projets en lien avec la cybersécurité :

- Proposition d'un RSSI mutualisé
- Accompagnement et conseil pour la mise en place de projets (utilisation du plan France Relance)
- Dans le cadre de la mutualisation et de la gestion des données (cf groupe mutualisation), fourniture d'une sauvegarde centralisée sur la collectivité.

La politique est de préconiser les bonnes actions, de rédiger des schémas directeurs, mais pas de prendre des responsabilités directes sur la sécurité.

RAPPORT SUR LE DEVELOPPEMENT DES USAGES

COMPTE RENDU D'AUDITION

I] Groupe de travail : CYBERSECURITE

Date de l'entretien : 18/05/2022

Agents présents : Pierre KREMER

Nom de la collectivité ou de l'organisme : CA du GRAND ANNECY

Personne contactée : Francoise RINGOT

Fonction dans la structure : Directrice des SYSTEMES D'INFORMATION ET DU NUMERIQUE

Tel : 04 50 63 48 80 / 06 79 91 39 78

Mail : fringot@grandannecy.fr

Site internet : https://www.grandannecy.fr/

Remarques :

La CA du GRAND ANNECY nous a partagé son expérience à la suite d'une attaque subie fin 2020. Cependant, il est à noter que les projets qu'elle a mis en place ne concernent que ses propres services. Aucun des membres de la CA n'est mutualisé informatiquement avec elle.

II] Avant l'audition

Projet mis en place par la collectivité : divers projets supposés, en conséquence d'une attaque par ransomware fin 2020

Singularité du projet : la singularité de la problématique est que la collectivité a dû faire face à d'importantes conséquences dues à la fuite de données, jusqu'à plusieurs mois après l'attaque.

RAPPORT SUR LE DEVELOPPEMENT DES USAGES

COMPTE RENDU D'AUDITION

III] Présentation de la collectivité

Statut juridique : communauté d'agglomération

Date de création : 2017

Périmètre d'action / membre : 34 communes, dont 20 communes de moins de 2 000 habitants et une ville-centre de plus de 130 000 habitants.

Nombre d'agents : 1200

Fonctionnement de la collectivité : RAS, pas de mutualisation informatique avec les membres

IV] Présentation du projet

Contexte politique de la mise en œuvre : attaque par rançongiciel

Description : plusieurs projets ont été imaginés pour réduire la surface d'attaque et améliorer la sécurité de la CA (cf le compte-rendu ci-après)

Schéma / structure juridique : les projets mis en place ne concernent que les propres services de la structure, et ne nécessitent donc aucune structure particulière.

Cout du projet : environ 130 000 € (mais contours flous entre investissement informatique classique, réponse à l'attaque, périmètre France Relance …)

Financement : Plan France Relance en complément du budget principal

Nombre d'agents en charge du projet et répartition par filière et grade : contour flou, car plusieurs projets sont mis en place, et concernent plusieurs services

Durée de lancement / initiation du projet : Janvier 2021

1. Avant l'attaque

La CA du GRAND ANNECY se considérait a priori comme très bien protégée. Elle possédait, avant l'attaque, deux salle blanches redondantes, ainsi que plusieurs sites de sauvegardes. Cependant, toutes ces protections n'avaient pour but que de cibler des dysfonctionnements matériels (pannes, incendies, inondations etc.). Le rançongiciel qui les a ciblés a malheureusement pu se faufiler dans l'ensemble du système.

2. Description de l'attaque par rançongiciel

L'attaque a été très particulière, car elle a eu lieu le 27 décembre, et n'a été découverte qu'en janvier. En la constatant, la décision a été prise immédiatement d'éteindre l'ensemble du parc informatique, ainsi que les serveurs, et d'appeler l'ANSSI. Cette dernière les a renvoyés vers une liste de prestataires qualifiés, et la CA a choisi Orange Cyberdéfense.

Le parc informatique a été « désinfecté », et un autre prestataire tiers (DATA BACK à la Roche-Sur-Yon) a réussi à récupérer la totalité des données cryptées par le virus.

L'incident a donc été traité de manière très rapide pour ce type d'attaque, car les paies de janvier (pour 1200 agents) ont pu être faites quasiment normalement, pour exemple. Les autres services ont été rétablis au fur et à mesure. La CA souhaite appuyer sur un élément très important, qui est le Plan de Reprise d'Activité, et en particulier sur les priorisations qu'il contient. En effet, le travail de reprise a été très perturbé par les sollicitations continuelles des différents services qui fonctionnaient en mode dégradé. Un PRA donne une feuille de route précise et objective, et permet de couper tout tentative de « shuntage » d'un processus déjà très compliqué.

Toutes les attaques n'ont malheureusement pas une issue aussi favorable. Plusieurs facteurs spécifiques ont permis à la collectivité de se relever facilement :

- Paradoxalement, le fait d'avoir été à l'arrêt complet les a dissuadés de restaurer trop vite leurs sauvegardes, et donc de « réinstaller » le virus. Il s'agissait donc d'un mal pour un bien, car chaque attaque nécessitant un temps, et une analyse détaillée pour éviter de laisser des éléments vérolés dans les systèmes
- Le rançongiciel utilisé n'a crypté que le début des disques durs. Cela en empêchait la lecture (ils étaient notés comme vides ou à formater), mais les données derrière la table des matières n'avaient pas été écrasées. C'est cette particularité qui a permis à DATA BACK de restaurer toutes les bases et tous les fichiers.

Pour information, la source de l'attaque était un phishing par courriel : un agent a malheureusement donné ses identifiants et mots de passe. D'après Orange Cyberdéfense, le pirate a alors pu s'escalader « administrateur » en changeant les droits d'un script (exploitation d'une faille alors ouverte sur la gestion Active Directory de Microsoft), et a ensuite pu petit à petit prendre le contrôle de toute la structure, y compris des sauvegardes.

3. Projets engagés en parallèle

La collectivité a mis en place plusieurs projets relatifs à la cybersécurité suite à cette attaque. Comme déjà précisé, il est à noter que ces projets ne concernent que ses propres services.

- Les agents ne sont plus administrateurs des postes (mais cela implique plus de travail de gestion des postes au quotidien)
- Tous les mots de passe ont été changé, en veillant à ce qu'ils soient uniques et assez sécurisés
- Certains points critiques de la structure informatiques ont été coupés de l'extérieur (en conséquence, il est nécessaire d'intervenir physiquement pour la gestion de certains serveurs)
- Un processus de silotage a été mis en place (création de VLAN étanches, et séparation d'une manière générale de toutes les fonctions)

- Lancement de fausses campagnes de phishing. Pour information, alors que la première a eu lieu 15 jours après une autre attaque, cette fois-ci de la ville d'Annecy, 25% des agents ont cliqué, 13% ont donné leur identifiants et mots de passe.
- Mise en place de campagnes par mail et de formations
- Mise en place de MFA (authentification multifactorielle : un accès doit être validé par SMS par exemple) pour l'accès VPN (virtual private network : accès au réseau à distance, comme dans le cas du télétravail)
- Equipement des agents en masse avec des mobiles, monitorés par la solution DUO (gestion des terminaux et de leur sécurité à distance)
- Utilisation du Plan France Relance :
    - 50 000€ pour 2021, 40 000€ pour 2022
    - Pour information, il n'y a pas encore eu de vérification sur les prestations réalisées, mais une exigence que la collectivité engage un budget complémentaire, au moins sur une partie des travaux.
    - Mise en place d'un bastion WALLIX (pour la gestion des accès)
    - Protection des données avec NETWRIX
    - Arrivée d'un RSSI (engagement obligatoire pour le Plan France Relance, même si c'est à travers une prestation externe)
    - Assistance pour rédiger un PRA complet, mais aussi les procédures de fonctionnement
    - Mise en place de Sentinel ONE (EDR - Endpoint Detection & Response, qui est une solution de surveillance active de l'informatique) monitoré par un prestataire

4. Bilan

La CA du GRAND ANNECY est souvent sollicitée par d'autres collectivités, qui l'interrogent sur la cybersécurité. Elle conseille bien évidemment de mettre en place des solutions de protection par anticipation, en soulignant qu'il ne s'agit pas simplement de projets ponctuels, mais bien d'un processus qui doit être renouvelé en continu, une amélioration globale des protections entraînant systématiquement une sophistication des attaques...

RAPPORT SUR LE DEVELOPPEMENT DES USAGES

COMPTE RENDU D'AUDITION

I] Groupe de travail : CYBERSECURITE

Date de l'entretien : 17 novembre 2021

Agents présents : Jamal BAINA

Nom de la collectivité ou de l'organisme : ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)

Personne contactée : M. Michel ROCHELET

Fonction dans la structure : Délégué à la sécurité numérique pour la région Grand Est

Tel : 06 45 23 42 75

Mail : michel.Rochelet@ssi.gouv.fr

Site internet : https://www.ssi.gouv.fr/

Remarques :

L'ANSSI est un service d'état qui a été créé dans le but d'améliorer la sécurité informatique en France. Cette audition ne peut donc pas être lue comme celle d'une autre collectivité, dont MOSELLE FIBRE pourrait directement s'inspirer pour ses propres projets.

II] Avant l'audition

Projet mis en place par la collectivité :
- la veille et la réaction,
- le développement de produits,
- l'information et le conseil,
- la formation,
- la labellisation de produits et de prestataires de confiance

Singularité du projet : l'ANSII est l'organisme national central de la thématique cybersécurité

RAPPORT SUR LE DEVELOPPEMENT DES USAGES

COMPTE RENDU D'AUDITION

III] Présentation de la collectivité

Statut juridique : l'Agence Nationale de la Sécurité des Systèmes d'Information est un service français créé par décret

Date de création : juillet 2009

Périmètre d'action / membre : périmètre d'action national / pas de membre

Nombre d'agents : environ 600 agents

Fonctionnement de la collectivité : il ne s'agit pas d'une collectivité, mais d'un service d'état

IV] Présentation du projet

Contexte politique de la mise en œuvre : pas de contexte particulier.

Description :

- Rapports et Recommandations,
- Qualification des produits, services et prestations
- Guides Méthodologique recommandés pour l'Analyse des Risques, Homologation des dispositifs et protections mises en place, Politique Sécurité Système d'Information.
- Accompagnement, conseil et sensibilisation des acteurs concernés dans leurs démarches SSI
- Financement de Projets de Mise en place ou Consolidation SSI (70% ANSSI, 30% Porteurs pour des budget projets jusqu'à 100 k€)

Schéma / structure juridique : l'ANSSI est un service d'état.

Cout du projet : ne s'agissant pas d'un projet particulier, il est proposé pour information le budget moyen annuel de la structure, qui est d'environ 21 millions d'euros hors masse salariale.

Financement : par l'état

Nombre d'agents en charge du projet et répartition par filière et grade : environ 700 agents

Durée de lancement / initiation du projet : 2009

RAPPORT SUR LE DEVELOPPEMENT DES USAGES

COMPTE RENDU D'AUDITION

Pour information, le résumé de l'entretien de Jamal, dans le cadre de la vidéoprotection :

1. Actions de l'ANSSI

L'ANSSI accompagne les services publics, les Collectivités et les Entreprises sur la Sécurité des Systèmes d'Information :

- Rapports et Recommandations,
- Qualification des produits, services et prestations
- Guides Méthodologique recommandés pour l'Analyse des Risques, Homologation des dispositifs et protections mises en place, Politique Sécurité Système d'Information.
- Accompagnement, conseil et sensibilisation des acteurs concernés dans leurs démarches SSI
- Financement de Projets de Mise en place ou Consolidation SSI (70% ANSSI, 30% Porteurs pour des budget projets jusqu'à 100 k€)

Par contre, l'ANSSI ne certifie pas la Sécurité des SI, d'architectures ni dispositifs mis en œuvre par les acteurs. Elle accompagne et recommande les bonnes pratiques et oriente vers des prestataires qualifiés.

2. Sensibilisation SSI par l'ANSSI

M. Rochelet, s'est proposé pour intervenir lors d'un séminaire Sensibilisation Sécurité des Systèmes d'Information ANSSI (2 Heures), organisé par MF visant une audience qualifiée de responsables SI, de décideurs et d'Elus. 30 à 50 participants. Le contenu est plus généraliste et moins technique mais il peut être adapté selon les participants, en 2 heures : Etat de la menace SSI, Comment organiser la démarche de Sécurité des SI, Méthodologies, Résultats.

A la suite du Séminaire de sensibilisation, des sollicitations particulières des participants peuvent être étudiées par l'ANSSI dans le cadre de ses actions d'accompagnement.

Dans le cadre d'une action collective SSI sous forme de Projet : Audit, remise à niveau, consolidation, mutualisation de ressources et des dispositifs, MF ou un groupement de ses membres pourraient être éligibles à un financement France Relance 70-30.

3. Présentation MOSELLE FIBRE

J. BAINA a effectué la présentation : Expérimentation Vidéoprotection et Mutualisation des Dispositifs et des Services

- Vidéoprotection : Dispositifs Techniques et Services Associés,
- Cas 1 : Dispositifs, Services et Ressources Non Mutualisés,
- Cas 2 : Mutualisation Dispositifs et Services : Réseau Fermé Dédié,
- Agence Nationale de la Sécurité des Système de l'Information ANSII : Recommandations et Qualification,
- Cas 3 : Mutualisation Dispositifs et Services : Réseau Ouvert Sécurisé.
- Finalement le dispositif retenu pour l'Expérimentation : Sans Mutualisation vidéoprotection et Analyse IA.
- Le Cas 3 serait envisageable dans une éventualité de nouveau positionnement de MF comme opérateur de dispositifs et de services vidéoprotection pour le compte des collectivités.

4. Recommandations ANSSI

M. Rochelet : En effet, les solutions Stormshield répondent aux exigences de Qualification de l'ANSSI. Cependant, les utiliser ne suffit pas. Il faut mettre en place toute une démarche et organisation et méthodologie de sécurisation des dispositifs de vidéoprotection. Stormshield peut aussi accompagner Moselle Fibre dans toutes les étapes nécessaires de l'architecture aux mesures opérationnelles de protection des dispositifs.

Il faut considérer tout dispositif de vidéoprotection comme un Système d'Information et lui appliquer les solutions et méthodologies recommandées par l'ANSSI.

- Effectuer une **Homologation de la Sécurité du Système d'Information**.
- Un Guide d'Homologation est proposé sur le site web de l'ANSSI.
- Il s'agit d'une Action Formelle qui Couvre Juridiquement la Responsabilité de l'Opérateur.
- Elle peut être effectuée en interne ou par un prestataire Externe (10 homme.Jours).
- En plusieurs étapes elle permet de :
  - Déterminer le Périmètre d'actions,
  - Analyser les Risques,
  - Identifier les mesures à mettre en place
  - Lister le Plan d'actions et le réaliser
  - Et enfin éditer un Document (10 pages : PSSI : Politique de Sécurité du Système d'Information. Ce document, équivalent à un Référentiel d'Audit, adressant aussi bien les aspects managériaux, organisationnels, que techniques.

M. Rochelet se propose d'accompagner Moselle Fibre dans la démarche selon les besoins, pour l'étape de l'Expérimentation ou pour une réflexion plus élargie vers les futurs projets.

Rapport sur le développement des usages

Moselle fibre
Réseau et Services

CYBERSECURITE

1

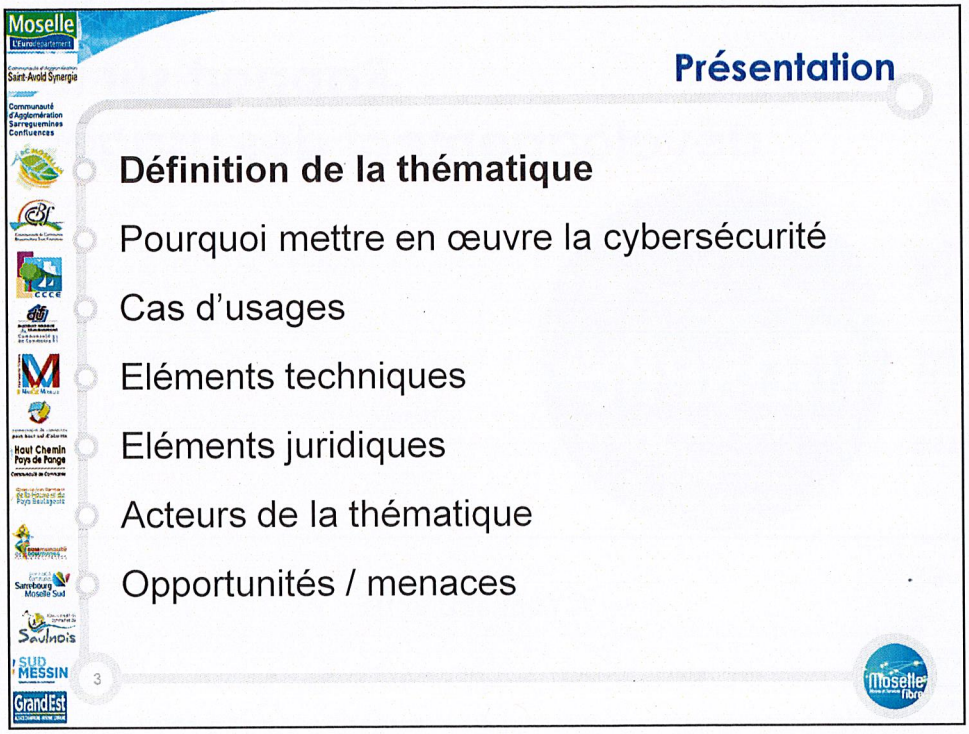
CYBERSECURITE

Présentation

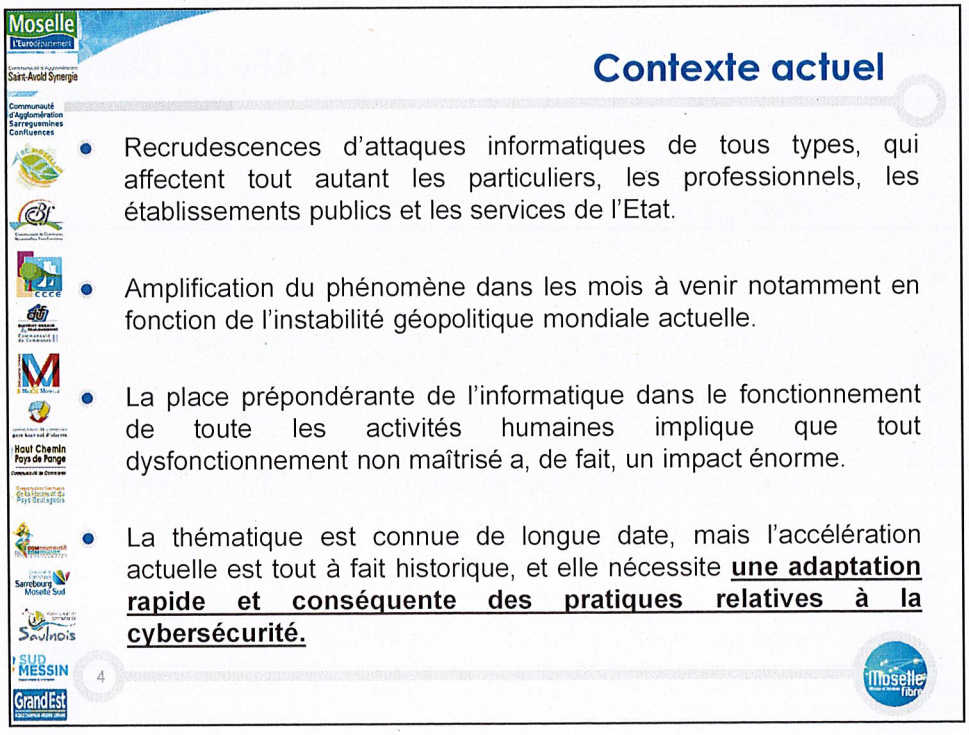
Retours d'expérience d'autres collectivités

Les actions potentielles de MOSELLE FIBRE

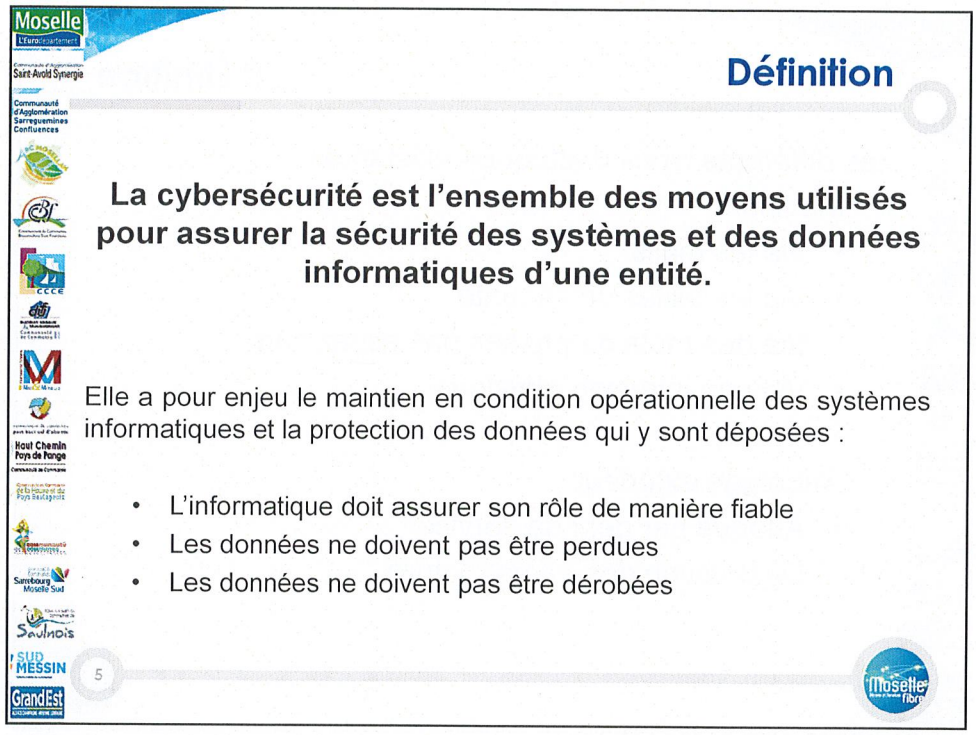
2


Présentation
Définition de la thématique
Pourquoi mettre en œuvre la cybersécurité
Cas d'usages
Eléments techniques
Eléments juridiques
Acteurs de la thématique
Opportunités / menaces
3

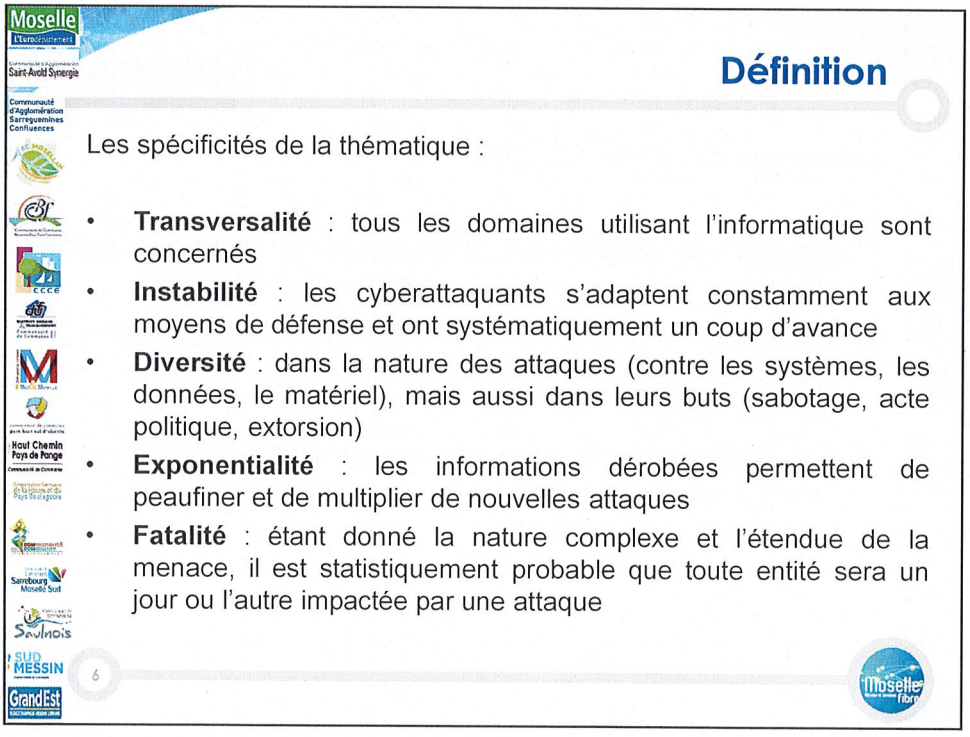
3


Contexte actuel
Recrudescences d'attaques informatiques de tous types, qui affectent tout autant les particuliers, les professionnels, les établissements publics et les services de l'Etat.
Amplification du phénomène dans les mois à venir notamment en fonction de l'instabilité géopolitique mondiale actuelle.
La place prépondérante de l'informatique dans le fonctionnement de toute les activités humaines implique que tout dysfonctionnement non maîtrisé a, de fait, un impact énorme.
La thématique est connue de longue date, mais l'accélération actuelle est tout à fait historique, et elle nécessite une adaptation rapide et conséquente des pratiques relatives à la cybersécurité.
4

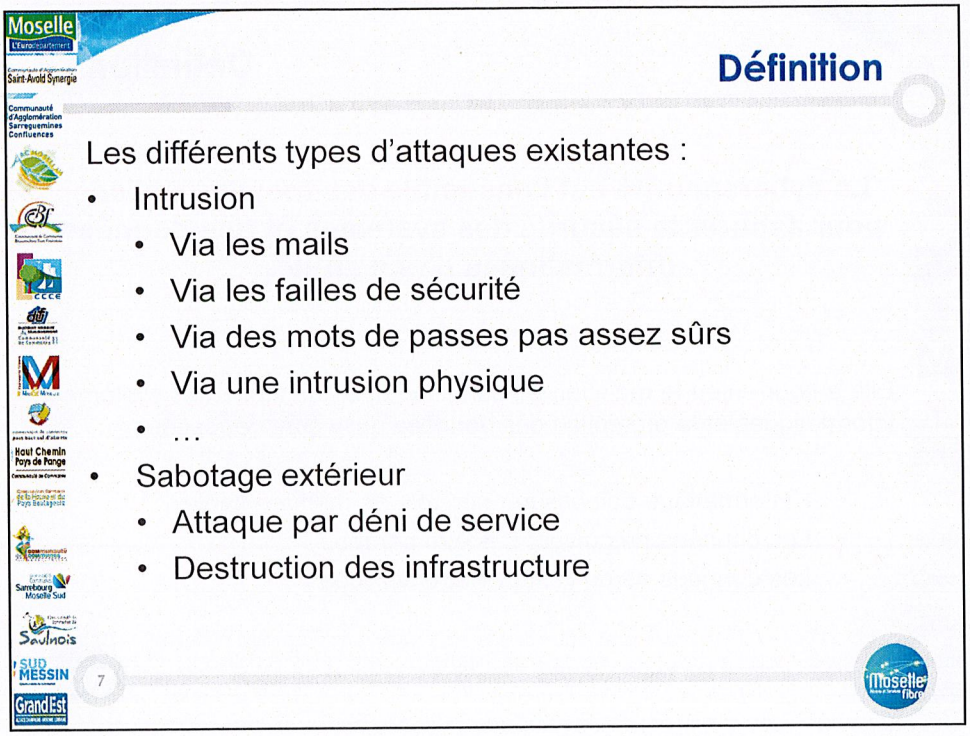
4


Définition
La cybersécurité est l'ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'une entité.
Elle a pour enjeu le maintien en condition opérationnelle des systèmes informatiques et la protection des données qui y sont déposées :
• L'informatique doit assurer son rôle de manière fiable
• Les données ne doivent pas être perdues
• Les données ne doivent pas être dérobées
5

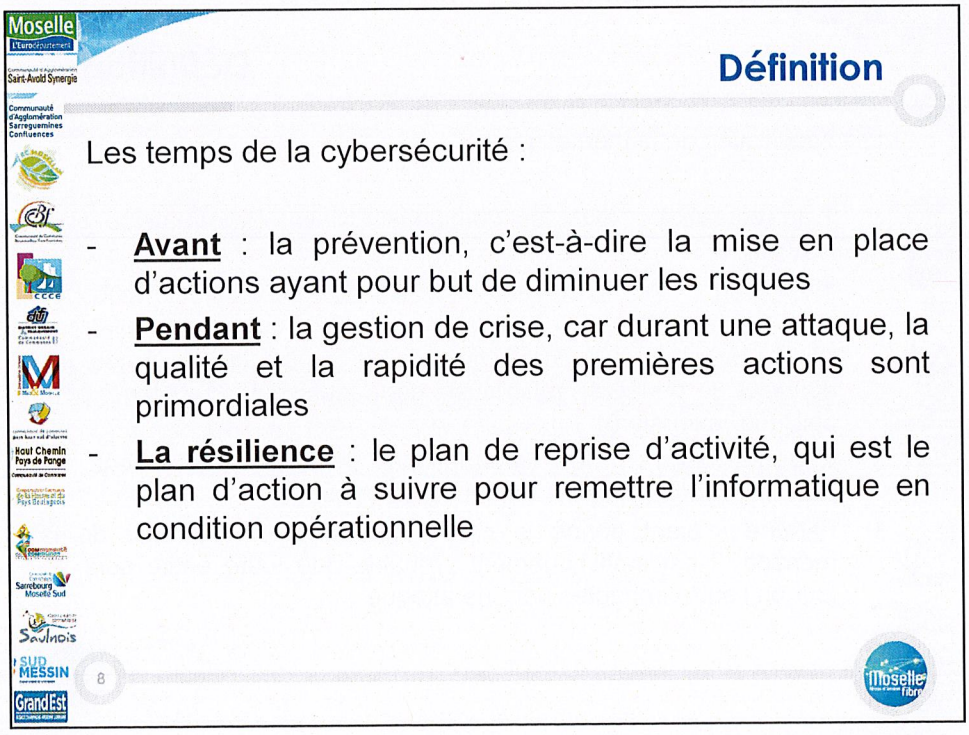
5


Définition
Les spécificités de la thématique :
• Transversalité : tous les domaines utilisant l'informatique sont concernés
• Instabilité : les cyberattaquants s'adaptent constamment aux moyens de défense et ont systématiquement un coup d'avance
• Diversité : dans la nature des attaques (contre les systèmes, les données, le matériel), mais aussi dans leurs buts (sabotage, acte politique, extorsion)
• Exponentialité : les informations dérobées permettent de peaufiner et de multiplier de nouvelles attaques
• Fatalité : étant donné la nature complexe et l'étendue de la menace, il est statistiquement probable que toute entité sera un jour ou l'autre impactée par une attaque
6

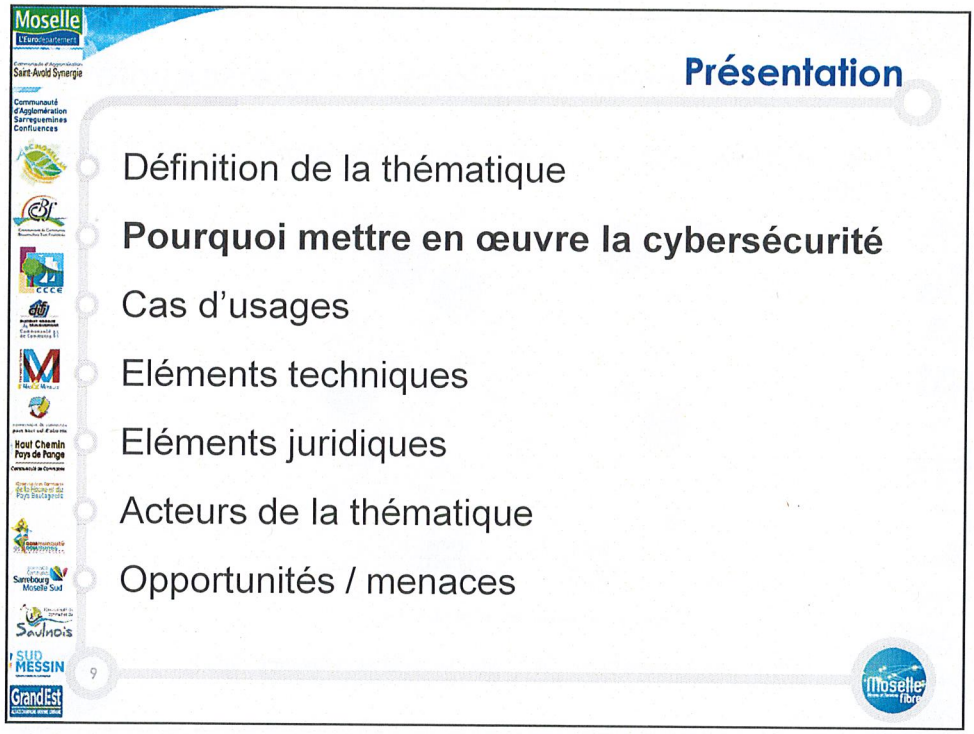
6


Définition
Les différents types d'attaques existantes :
• Intrusion
• Via les mails
• Via les failles de sécurité
• Via des mots de passes pas assez sûrs
• Via une intrusion physique
• …
• Sabotage extérieur
• Attaque par déni de service
• Destruction des infrastructure
7

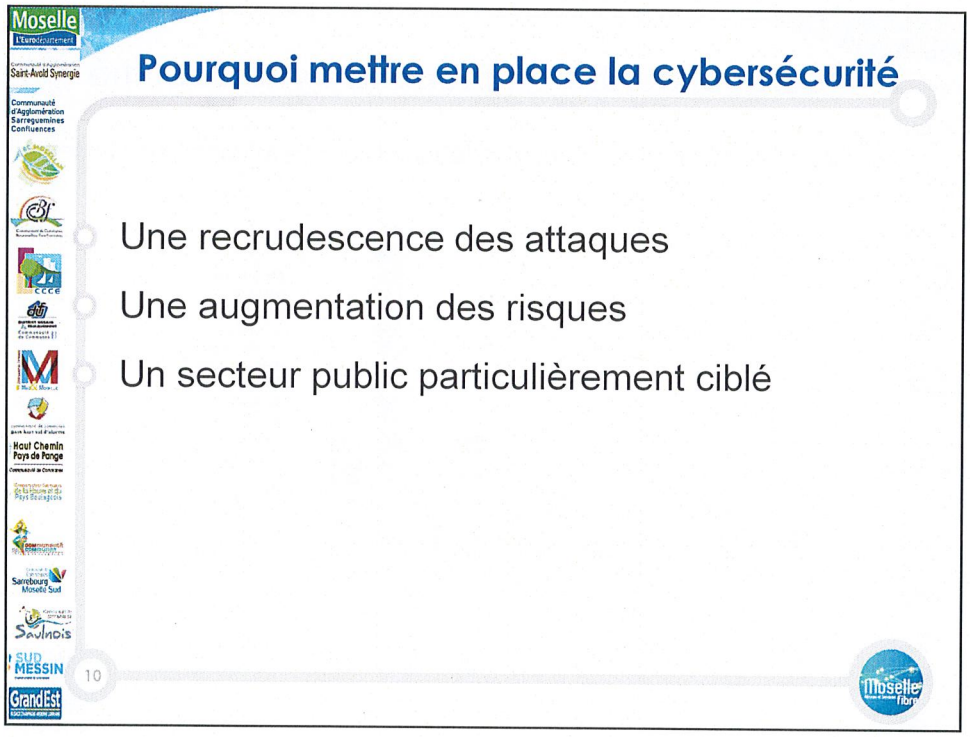
7


Définition
Les temps de la cybersécurité :
- Avant : la prévention, c'est-à-dire la mise en place d'actions ayant pour but de diminuer les risques
- Pendant : la gestion de crise, car durant une attaque, la qualité et la rapidité des premières actions sont primordiales
- La résilience : le plan de reprise d'activité, qui est le plan d'action à suivre pour remettre l'informatique en condition opérationnelle
8

8


Moselle
L'Eurodépartement
Présentation
Définition de la thématique
Pourquoi mettre en œuvre la cybersécurité
Cas d'usages
Eléments techniques
Eléments juridiques
Acteurs de la thématique
Opportunités / menaces
9

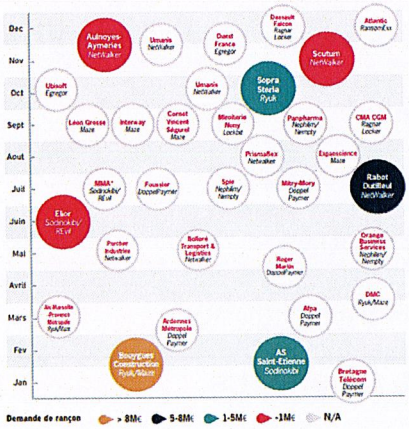
9


Moselle
L'Eurodépartement
Pourquoi mettre en place la cybersécurité
Une recrudescence des attaques
Une augmentation des risques
Un secteur public particulièrement ciblé
10

10

Pourquoi mettre en place la cybersécurité

Des extorsions donc les impacts sont sous-estimés (ici sur l'année 2020)



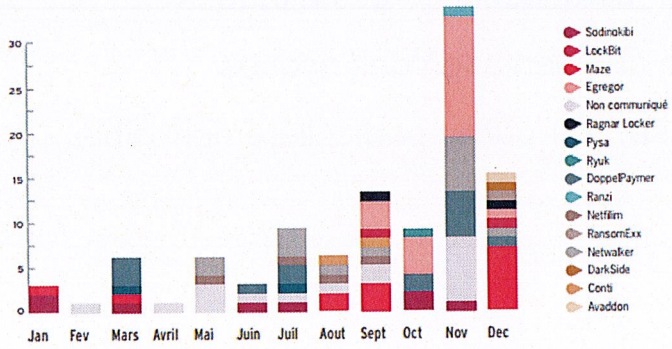
Crédit : Les Assises et EPITA – Cybersécurité et innovation (2020)

11

11

Pourquoi mettre en place la cybersécurité

Un écosystème parmi les cyberattaquants (ici l'évolution sur l'année 2020)



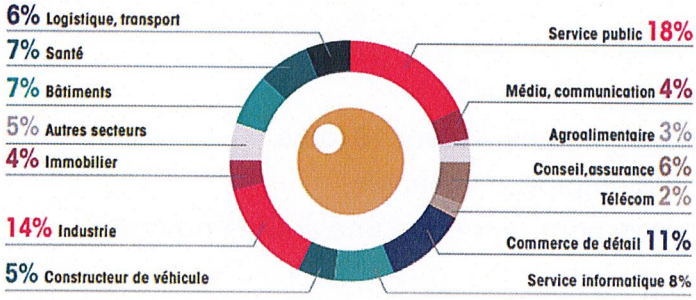
Crédit : Les Assises et EPITA – Cybersécurité et innovation (2020)

12

12

Pourquoi mettre en place la cybersécurité

Des victimes dans tous les secteurs d'activité, le service public étant la cible n°1 (données 2020)



Crédit : Les Assises et EPITA – Cybersécurité et innovation (2020)

13

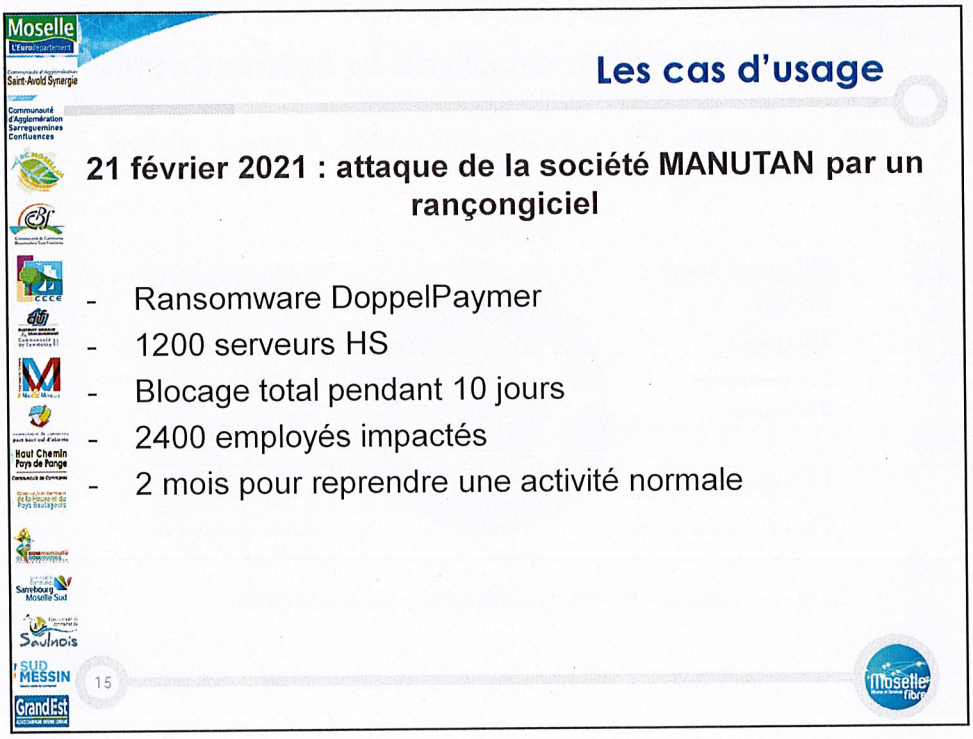
13

Présentation

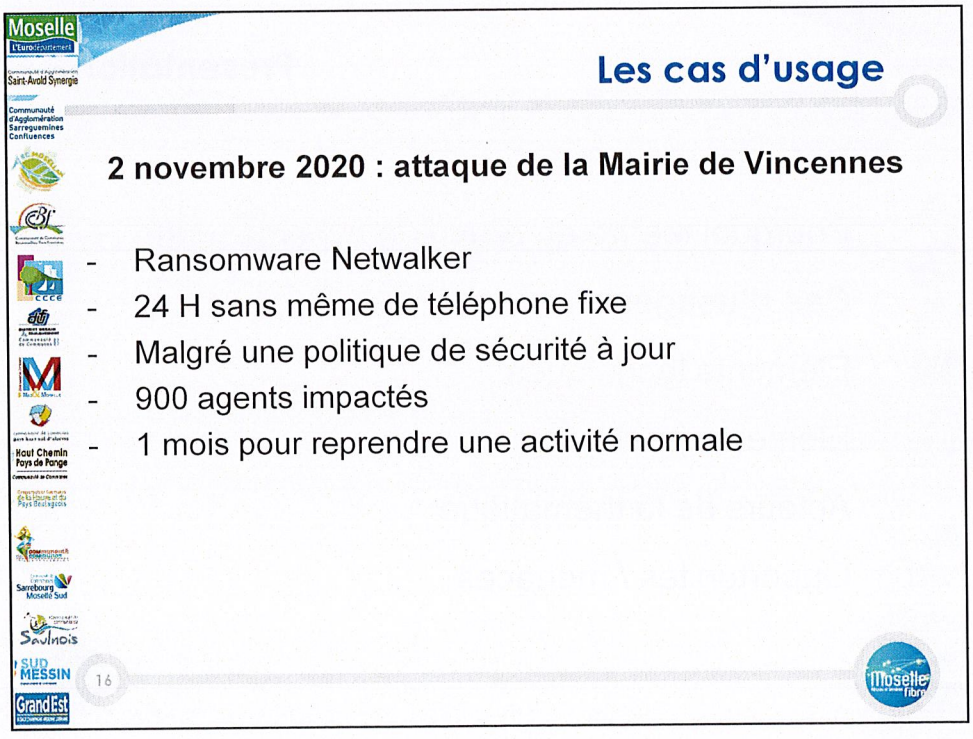
- Définition de la thématique
- Pourquoi mettre en œuvre la cybersécurité
- **Cas d'usages**
- Eléments techniques
- Eléments juridiques
- Acteurs de la thématique
- Opportunités / menaces

14

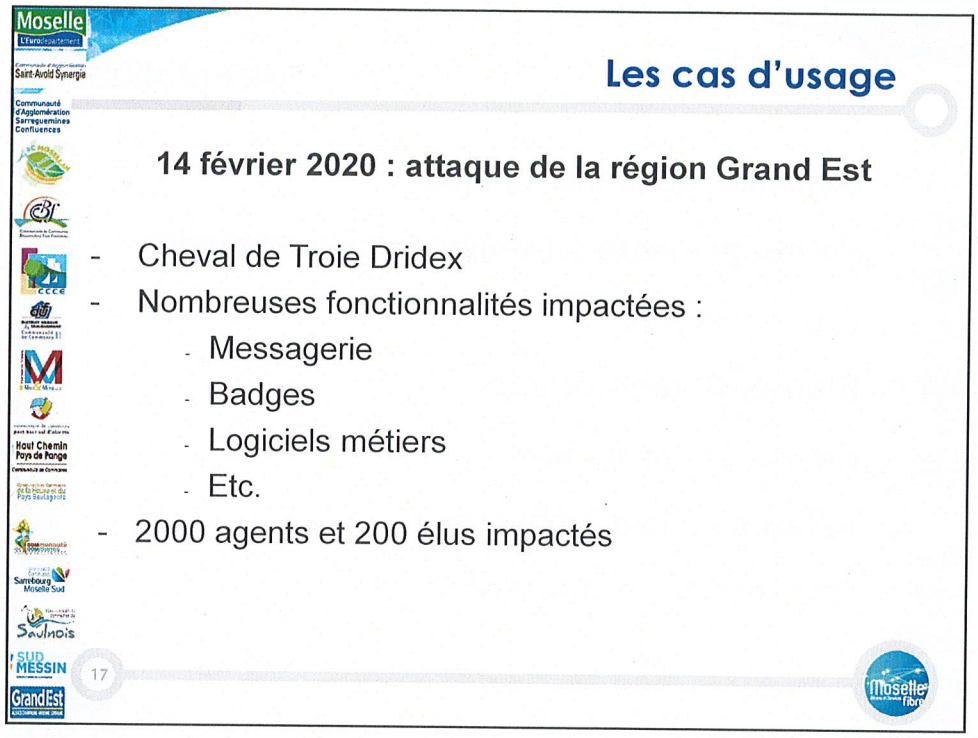
14


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
SaulNois
SUD MESSIN
GrandEst
Les cas d'usage
21 février 2021 : attaque de la société MANUTAN par un rançongiciel
- Ransomware DoppelPaymer
- 1200 serveurs HS
- Blocage total pendant 10 jours
- 2400 employés impactés
- 2 mois pour reprendre une activité normale
15
Moselle fibre

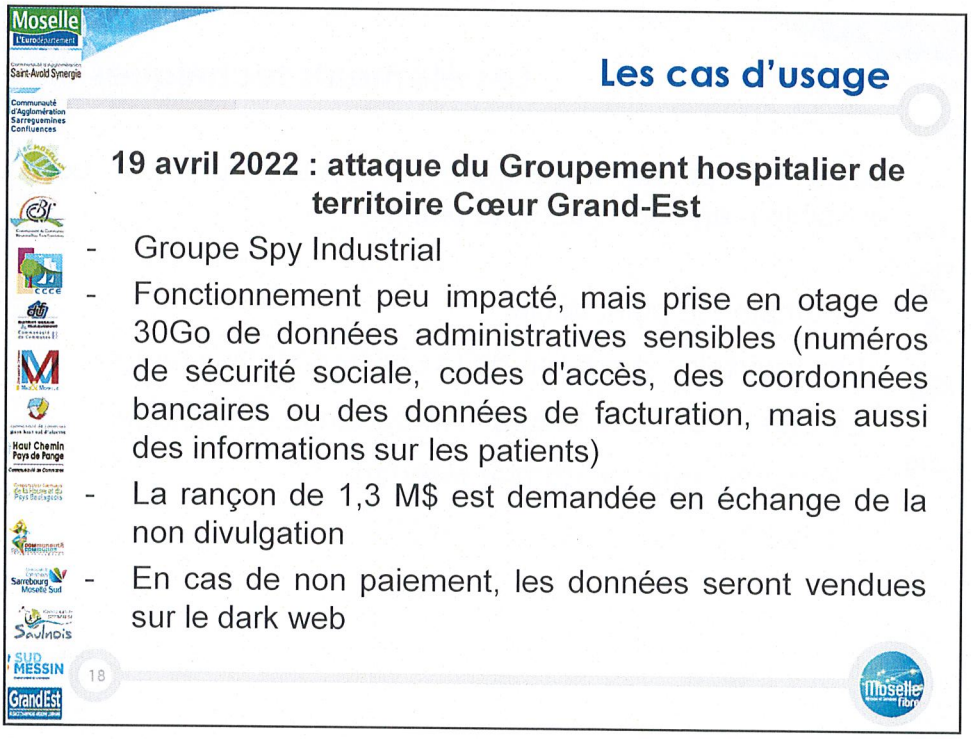
15


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
SaulNois
SUD MESSIN
GrandEst
Les cas d'usage
2 novembre 2020 : attaque de la Mairie de Vincennes
- Ransomware Netwalker
- 24 H sans même de téléphone fixe
- Malgré une politique de sécurité à jour
- 900 agents impactés
- 1 mois pour reprendre une activité normale
16
Moselle fibre

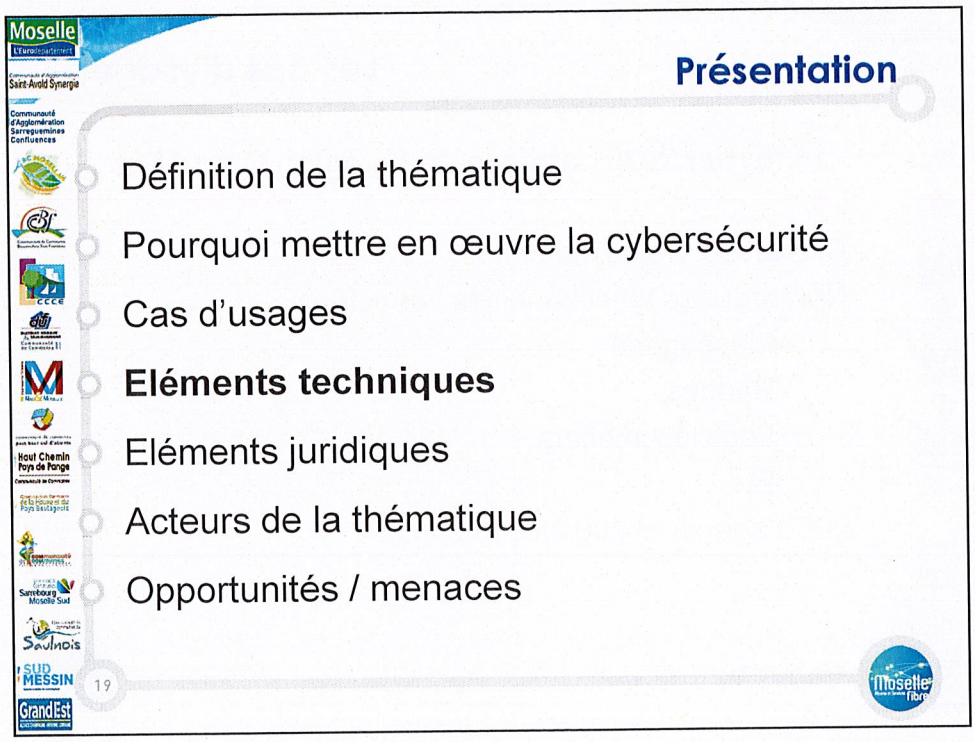
16


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
SUD MESSIN
GrandEst
Les cas d'usage
14 février 2020 : attaque de la région Grand Est
- Cheval de Troie Dridex
- Nombreuses fonctionnalités impactées :
- Messagerie
- Badges
- Logiciels métiers
- Etc.
- 2000 agents et 200 élus impactés
17
Moselle Fibre

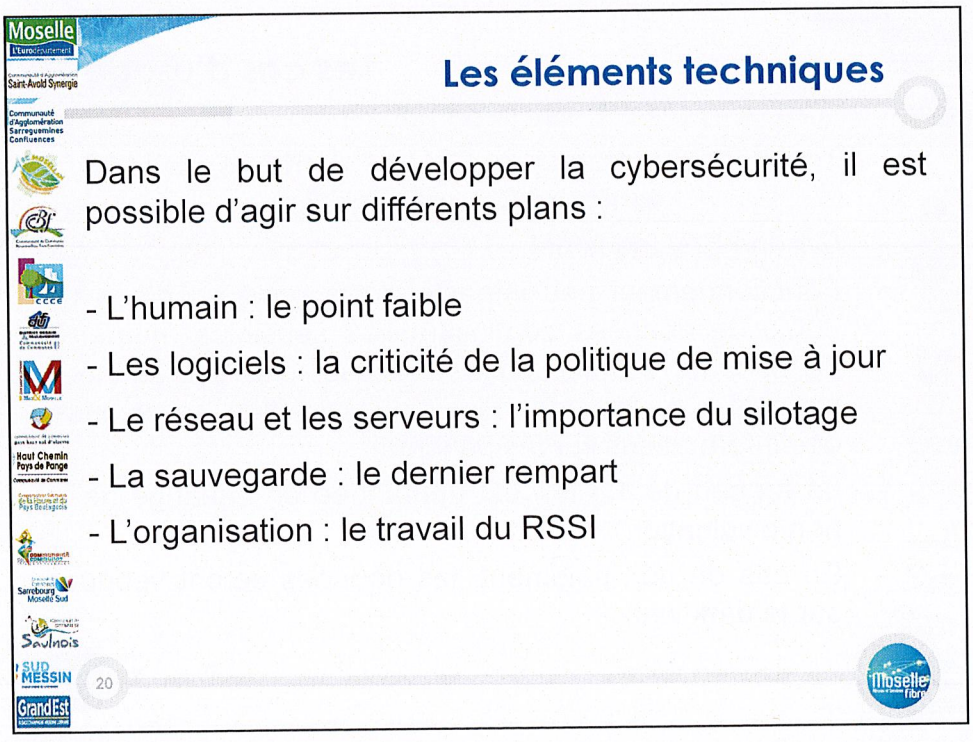
17


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
SUD MESSIN
GrandEst
Les cas d'usage
19 avril 2022 : attaque du Groupement hospitalier de territoire Cœur Grand-Est
- Groupe Spy Industrial
- Fonctionnement peu impacté, mais prise en otage de 30Go de données administratives sensibles (numéros de sécurité sociale, codes d'accès, des coordonnées bancaires ou des données de facturation, mais aussi des informations sur les patients)
- La rançon de 1,3 M$ est demandée en échange de la non divulgation
- En cas de non paiement, les données seront vendues sur le dark web
18
Moselle Fibre

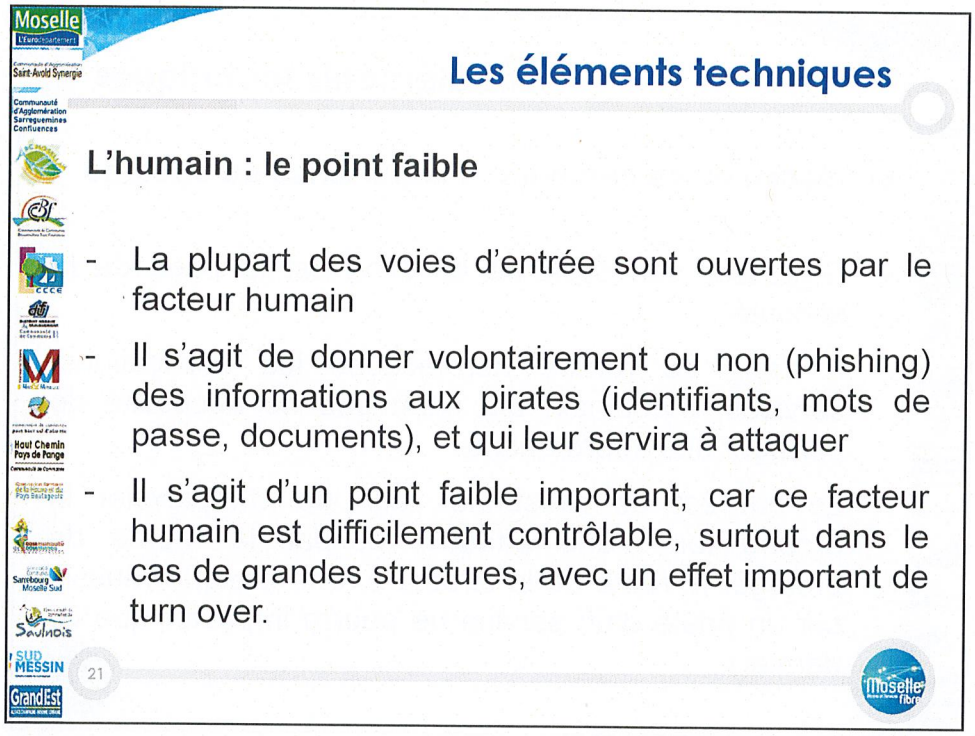
18


Moselle
L'Eurodépartement
Présentation
Définition de la thématique
Pourquoi mettre en œuvre la cybersécurité
Cas d'usages
Eléments techniques
Eléments juridiques
Acteurs de la thématique
Opportunités / menaces
19

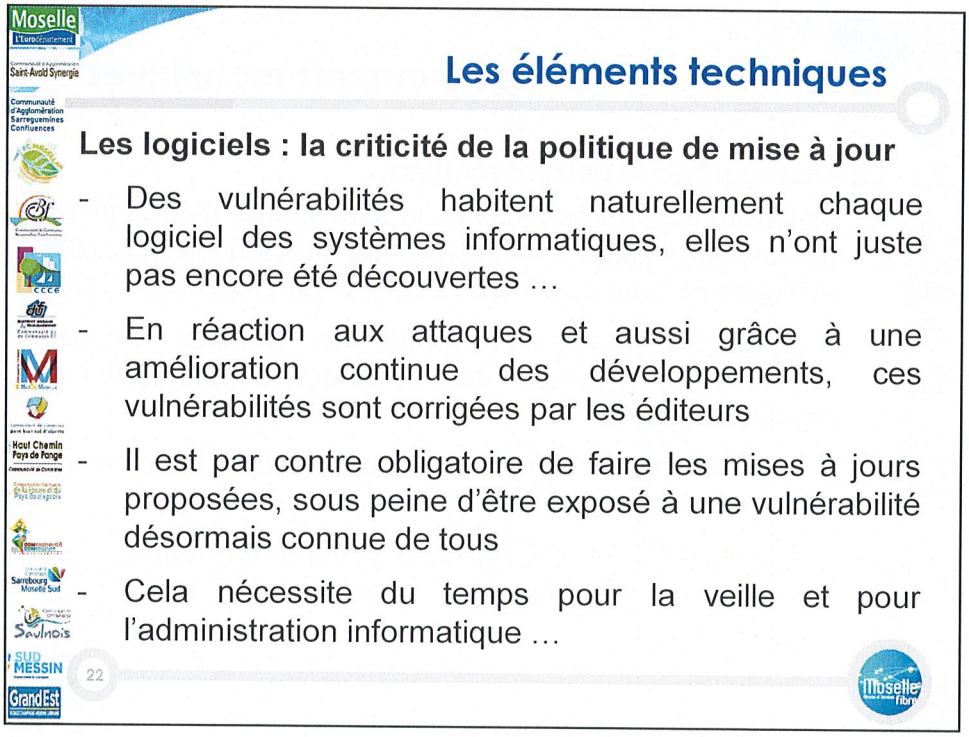
19


Moselle
L'Eurodépartement
Les éléments techniques
Dans le but de développer la cybersécurité, il est possible d'agir sur différents plans :
- L'humain : le point faible
- Les logiciels : la criticité de la politique de mise à jour
- Le réseau et les serveurs : l'importance du silotage
- La sauvegarde : le dernier rempart
- L'organisation : le travail du RSSI
20

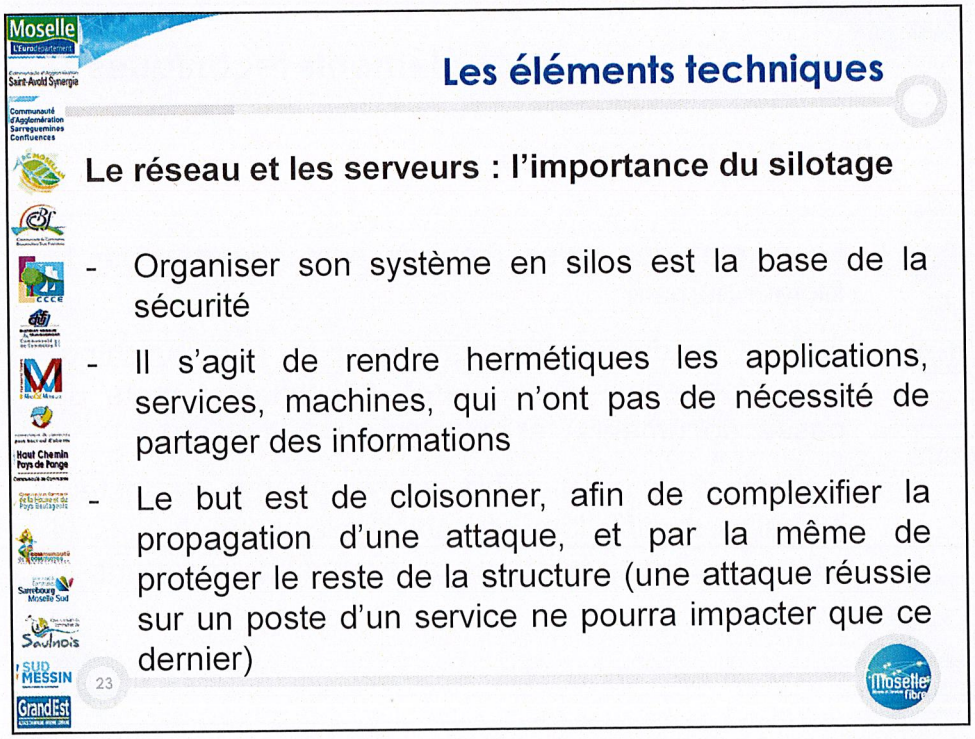
20


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
Saulnois
SUD MESSIN
GrandEst
Les éléments techniques
L'humain : le point faible
- La plupart des voies d'entrée sont ouvertes par le facteur humain
- Il s'agit de donner volontairement ou non (phishing) des informations aux pirates (identifiants, mots de passe, documents), et qui leur servira à attaquer
- Il s'agit d'un point faible important, car ce facteur humain est difficilement contrôlable, surtout dans le cas de grandes structures, avec un effet important de turn over.
21
Moselle fibre

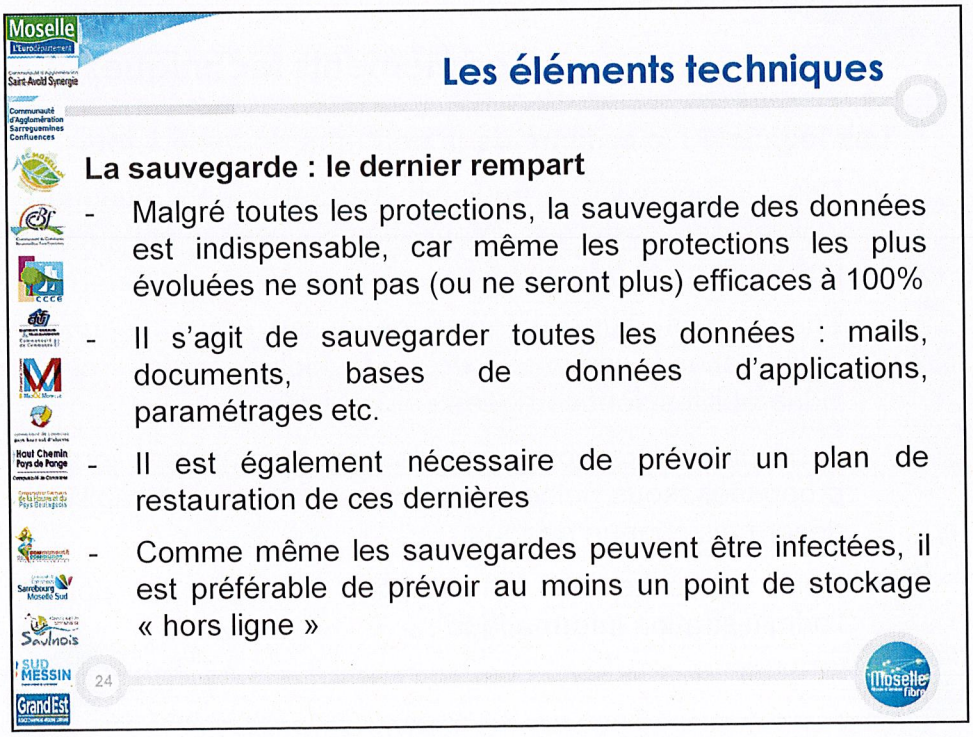
21


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
Saulnois
SUD MESSIN
GrandEst
Les éléments techniques
Les logiciels : la criticité de la politique de mise à jour
- Des vulnérabilités habitent naturellement chaque logiciel des systèmes informatiques, elles n'ont juste pas encore été découvertes …
- En réaction aux attaques et aussi grâce à une amélioration continue des développements, ces vulnérabilités sont corrigées par les éditeurs
- Il est par contre obligatoire de faire les mises à jours proposées, sous peine d'être exposé à une vulnérabilité désormais connue de tous
- Cela nécessite du temps pour la veille et pour l'administration informatique …
22
Moselle fibre

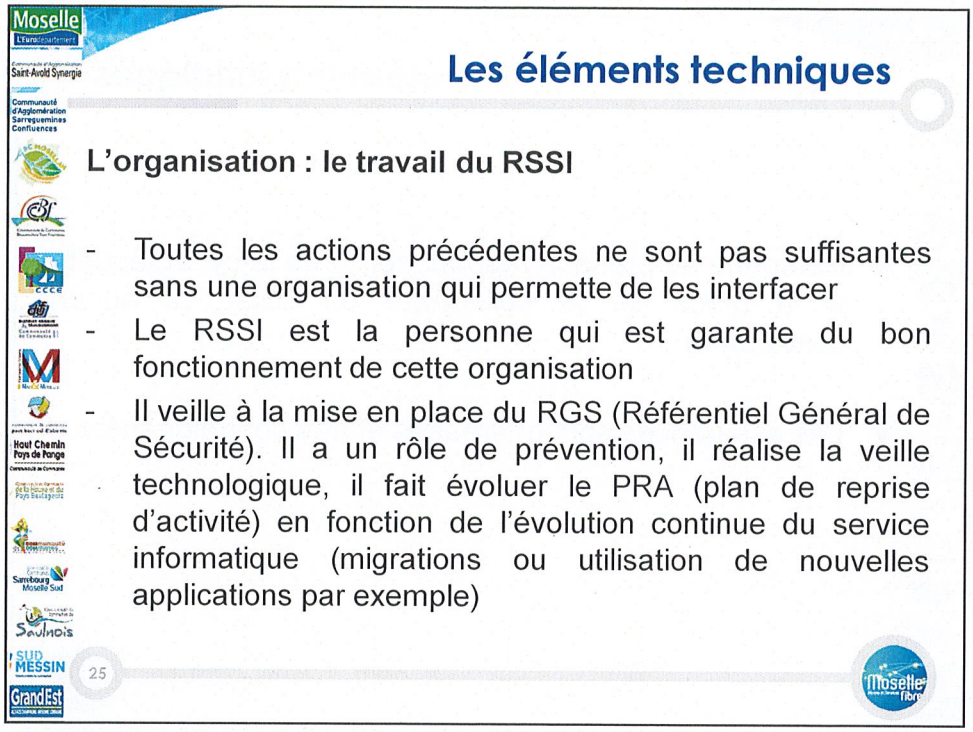
22


Les éléments techniques
Le réseau et les serveurs : l'importance du silotage
- Organiser son système en silos est la base de la sécurité
- Il s'agit de rendre hermétiques les applications, services, machines, qui n'ont pas de nécessité de partager des informations
- Le but est de cloisonner, afin de complexifier la propagation d'une attaque, et par la même de protéger le reste de la structure (une attaque réussie sur un poste d'un service ne pourra impacter que ce dernier)
23

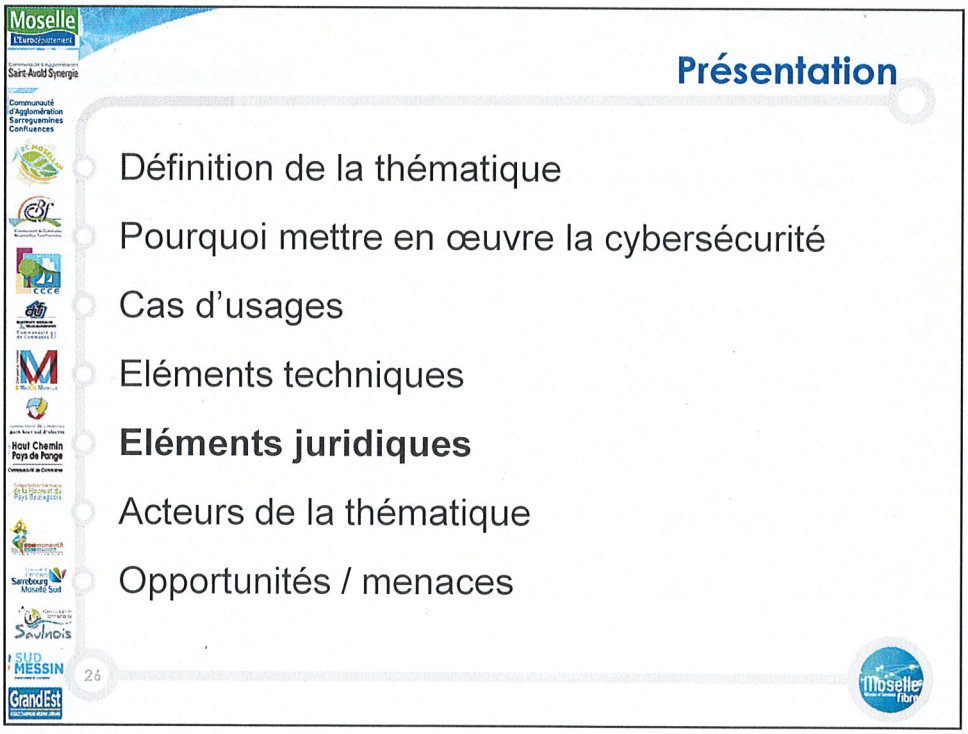
23


Les éléments techniques
La sauvegarde : le dernier rempart
- Malgré toutes les protections, la sauvegarde des données est indispensable, car même les protections les plus évoluées ne sont pas (ou ne seront plus) efficaces à 100%
- Il s'agit de sauvegarder toutes les données : mails, documents, bases de données d'applications, paramétrages etc.
- Il est également nécessaire de prévoir un plan de restauration de ces dernières
- Comme même les sauvegardes peuvent être infectées, il est préférable de prévoir au moins un point de stockage « hors ligne »
24

24


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Hauts Pays de Nancy
Hauts Pays de Nancy et du Pays Haut Val d'Alzette
Sarrebourg Moselle Sud
Saulnois
SUD MESSIN
GrandEst
Les éléments techniques
L'organisation : le travail du RSSI
- Toutes les actions précédentes ne sont pas suffisantes sans une organisation qui permette de les interfacer
- Le RSSI est la personne qui est garante du bon fonctionnement de cette organisation
- Il veille à la mise en place du RGS (Référentiel Général de Sécurité). Il a un rôle de prévention, il réalise la veille technologique, il fait évoluer le PRA (plan de reprise d'activité) en fonction de l'évolution continue du service informatique (migrations ou utilisation de nouvelles applications par exemple)
25
Moselle fibre

25


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Hauts Pays de Nancy
Hauts Pays de Nancy et du Pays Haut Val d'Alzette
Sarrebourg Moselle Sud
Saulnois
SUD MESSIN
GrandEst
Présentation
Définition de la thématique
Pourquoi mettre en œuvre la cybersécurité
Cas d'usages
Eléments techniques
Eléments juridiques
Acteurs de la thématique
Opportunités / menaces
26
Moselle fibre

26

Les éléments juridiques

- Personne ne prend la responsabilité de la cybersécurité à la place de la collectivité (ni l'Etat, ni aucun prestataire)
- Les assurances sont onéreuses et très contraignantes.

27

27

Présentation

Définition de la thématique

Pourquoi mettre en œuvre la cybersécurité

Cas d'usages

Eléments techniques

Eléments juridiques

Acteurs de la thématique

Opportunités / menaces

28

28

Les acteurs de la thématique

- L'Etat
- Les organismes de formation
- Les éditeurs de logiciels
- Les SS2I (société de services en ingénierie informatique)
- Les assureurs
- D'autres divers acteurs, suivant les initiatives (CDG, CCI, associations etc.)

29

29

Présentation

Définition de la thématique

Pourquoi mettre en œuvre la cybersécurité

Cas d'usages

Eléments techniques

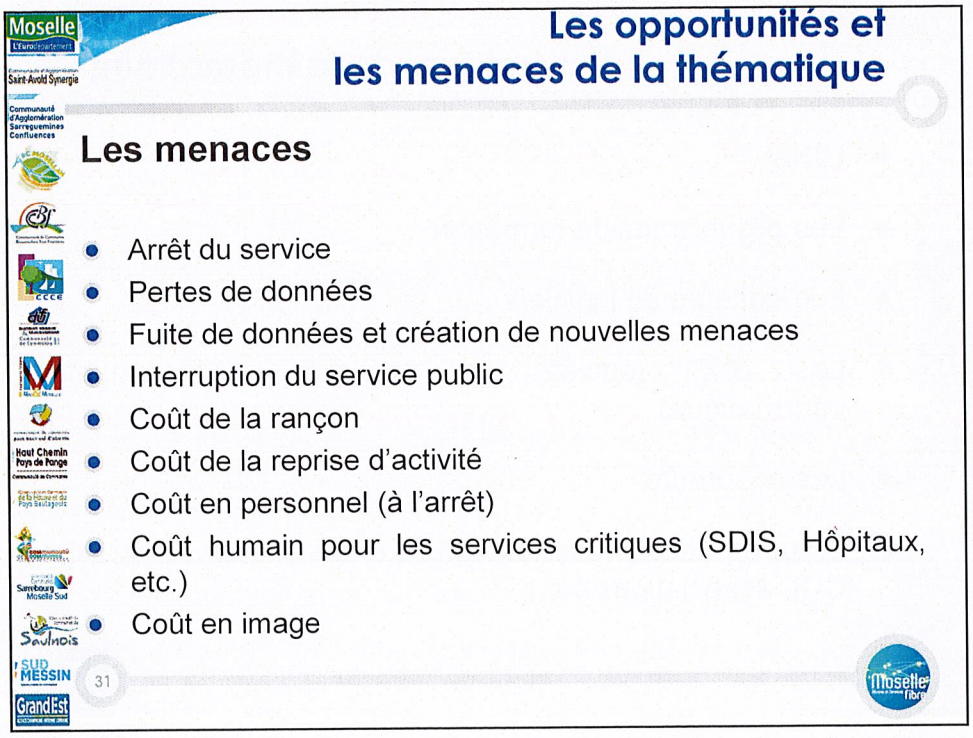
Eléments juridiques

Acteurs de la thématique

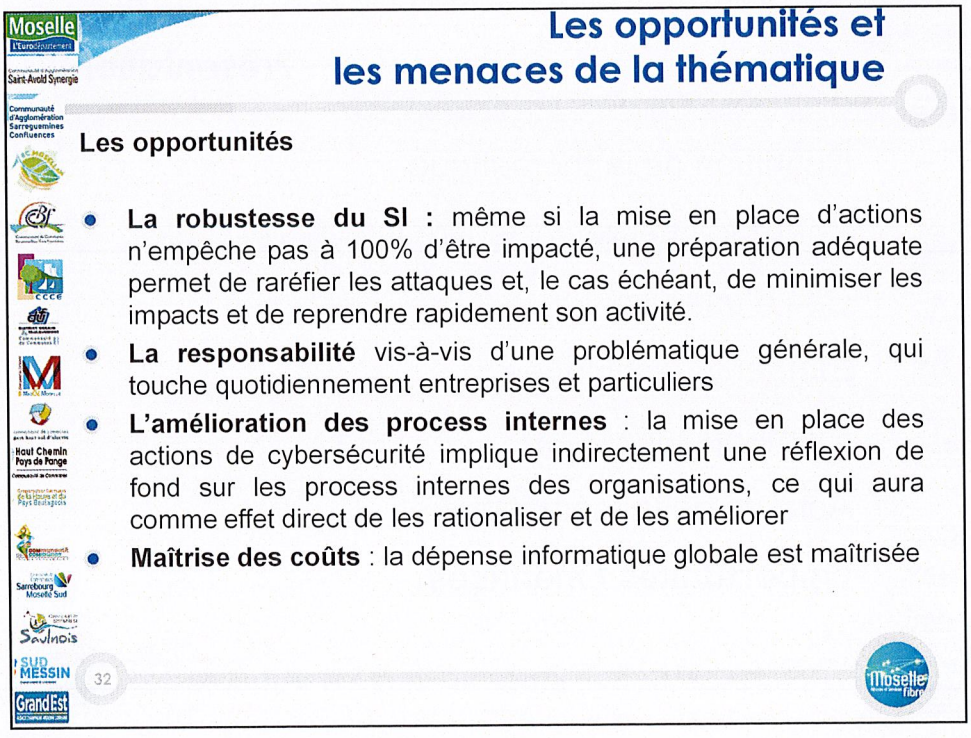
Opportunités / menaces

30

30


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
Saulnois
SUD MESSIN
Grand Est
Les opportunités et les menaces de la thématique
Les menaces
Arrêt du service
Pertes de données
Fuite de données et création de nouvelles menaces
Interruption du service public
Coût de la rançon
Coût de la reprise d'activité
Coût en personnel (à l'arrêt)
Coût humain pour les services critiques (SDIS, Hôpitaux, etc.)
Coût en image
31
Moselle Fibre

31


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
Saulnois
SUD MESSIN
Grand Est
Les opportunités et les menaces de la thématique
Les opportunités
La robustesse du SI : même si la mise en place d'actions n'empêche pas à 100% d'être impacté, une préparation adéquate permet de raréfier les attaques et, le cas échéant, de minimiser les impacts et de reprendre rapidement son activité.
La responsabilité vis-à-vis d'une problématique générale, qui touche quotidiennement entreprises et particuliers
L'amélioration des process internes : la mise en place des actions de cybersécurité implique indirectement une réflexion de fond sur les process internes des organisations, ce qui aura comme effet direct de les rationaliser et de les améliorer
Maîtrise des coûts : la dépense informatique globale est maîtrisée
32
Moselle Fibre

32

CYBERSECURITE

Présentation

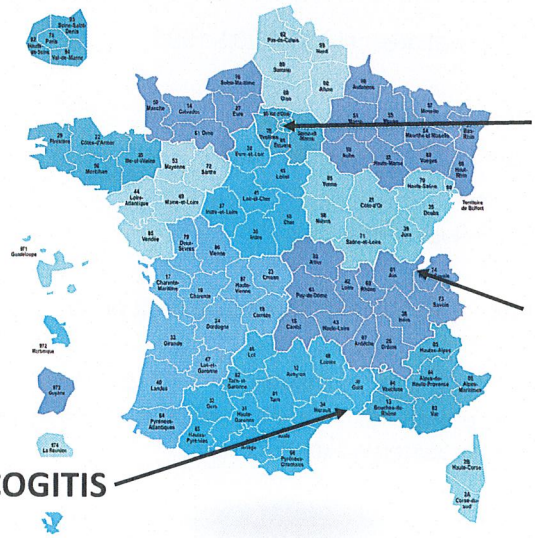
Retours d'expérience d'autres collectivités

Les actions potentielles de MOSELLE FIBRE

33

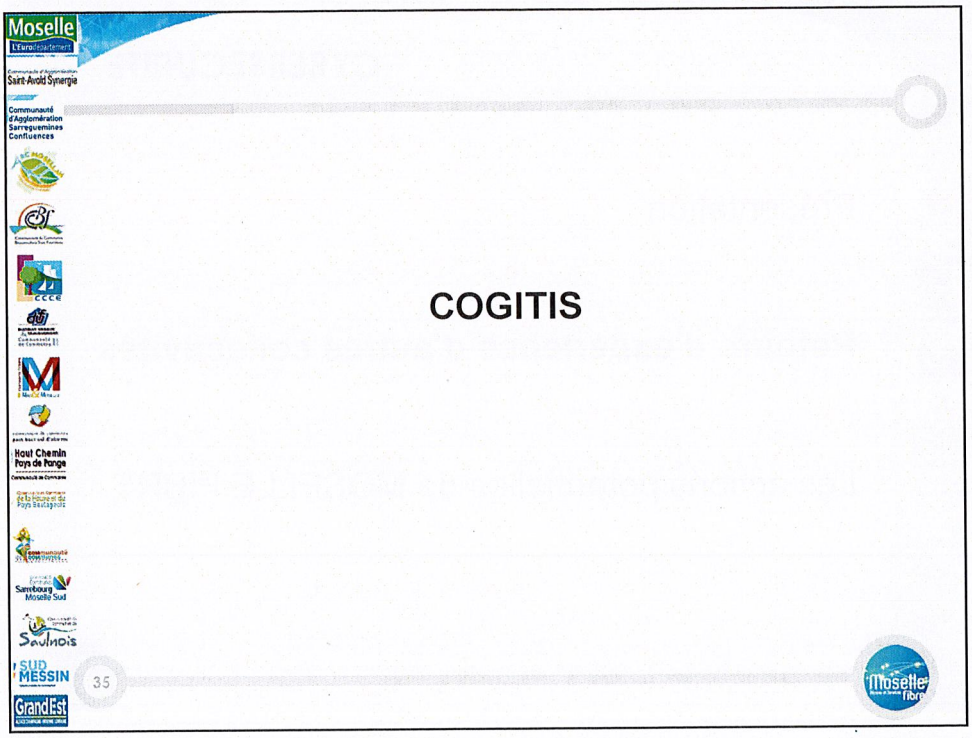
33

Les collectivités ayant mis en place des actions sur la cybersécurité

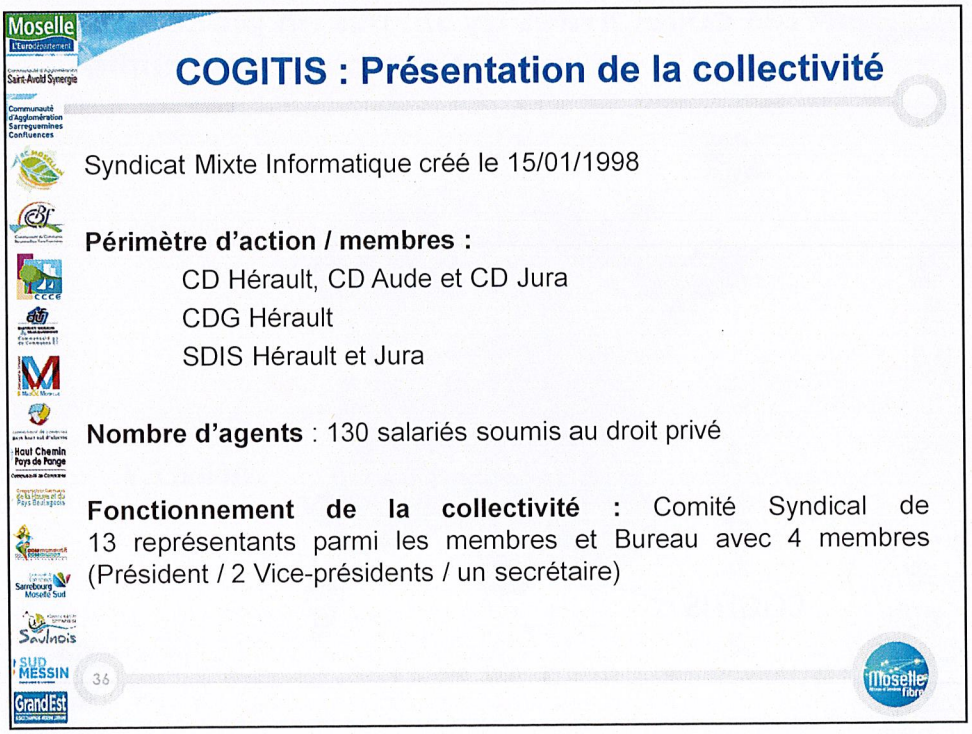


34

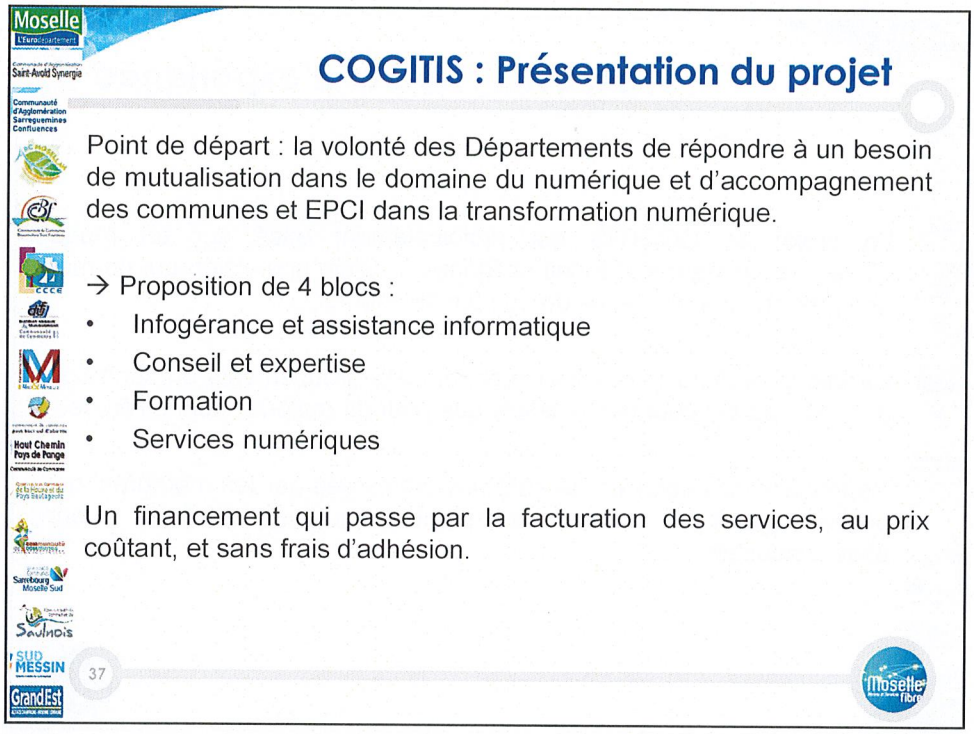
34


COGITIS
35

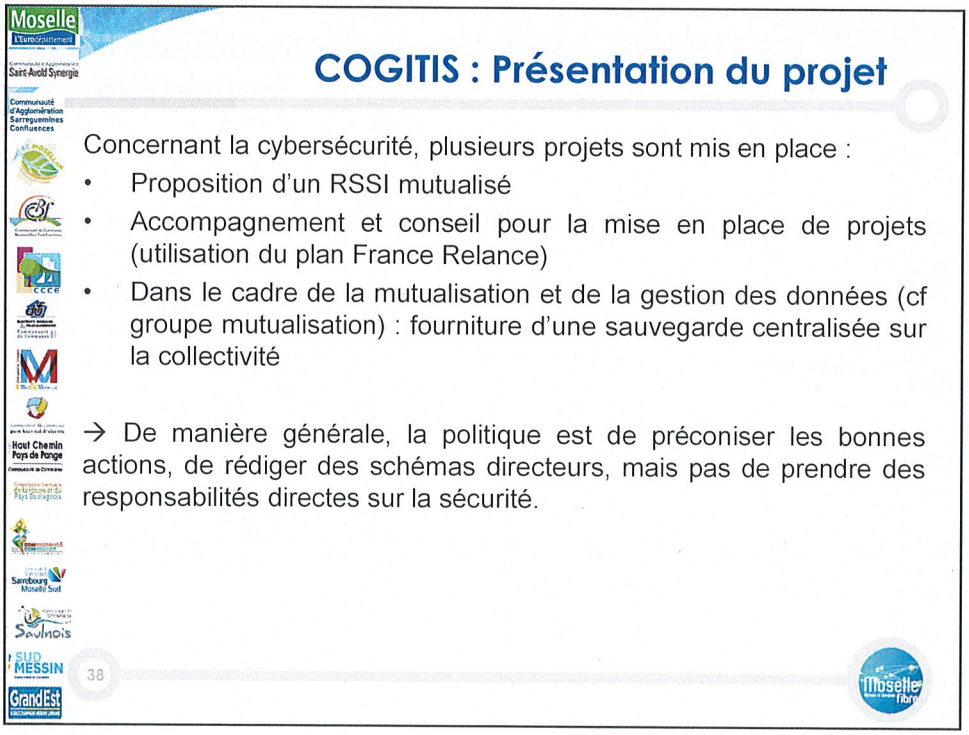
35


COGITIS : Présentation de la collectivité
Syndicat Mixte Informatique créé le 15/01/1998
Périmètre d'action / membres :
CD Hérault, CD Aude et CD Jura
CDG Hérault
SDIS Hérault et Jura
Nombre d'agents : 130 salariés soumis au droit privé
Fonctionnement de la collectivité : Comité Syndical de 13 représentants parmi les membres et Bureau avec 4 membres (Président / 2 Vice-présidents / un secrétaire)
36

36


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
SUD MESSIN
GrandEst
COGITIS : Présentation du projet
Point de départ : la volonté des Départements de répondre à un besoin de mutualisation dans le domaine du numérique et d'accompagnement des communes et EPCI dans la transformation numérique.
→ Proposition de 4 blocs :
• Infogérance et assistance informatique
• Conseil et expertise
• Formation
• Services numériques
Un financement qui passe par la facturation des services, au prix coûtant, et sans frais d'adhésion.
37
Moselle fibre

37


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
SUD MESSIN
GrandEst
COGITIS : Présentation du projet
Concernant la cybersécurité, plusieurs projets sont mis en place :
• Proposition d'un RSSI mutualisé
• Accompagnement et conseil pour la mise en place de projets (utilisation du plan France Relance)
• Dans le cadre de la mutualisation et de la gestion des données (cf groupe mutualisation) : fourniture d'une sauvegarde centralisée sur la collectivité
→ De manière générale, la politique est de préconiser les bonnes actions, de rédiger des schémas directeurs, mais pas de prendre des responsabilités directes sur la sécurité.
38
Moselle fibre

38

COGITIS : Retour d'expérience

Le projet de COGITIS est principalement basé sur un mode d'intervention léger « Conseil et Etudes ». C'est une vision qui permet une gestion simple et agile de son fonctionnement.

Certaines évolutions, qui impliqueraient des groupements ou centrales d'achats, autant pour des logiciels que pour du matériel, sont à l'étude.

Cependant, ces services ne sont pas plébiscités par les membres, qui préfèrent gérer eux-mêmes cette partie, et qui sont sensibles à leur bassin industriel.

39

39

CA GRAND ANNECY : Présentation de la collectivité

Communauté d'agglomération créée en 2017

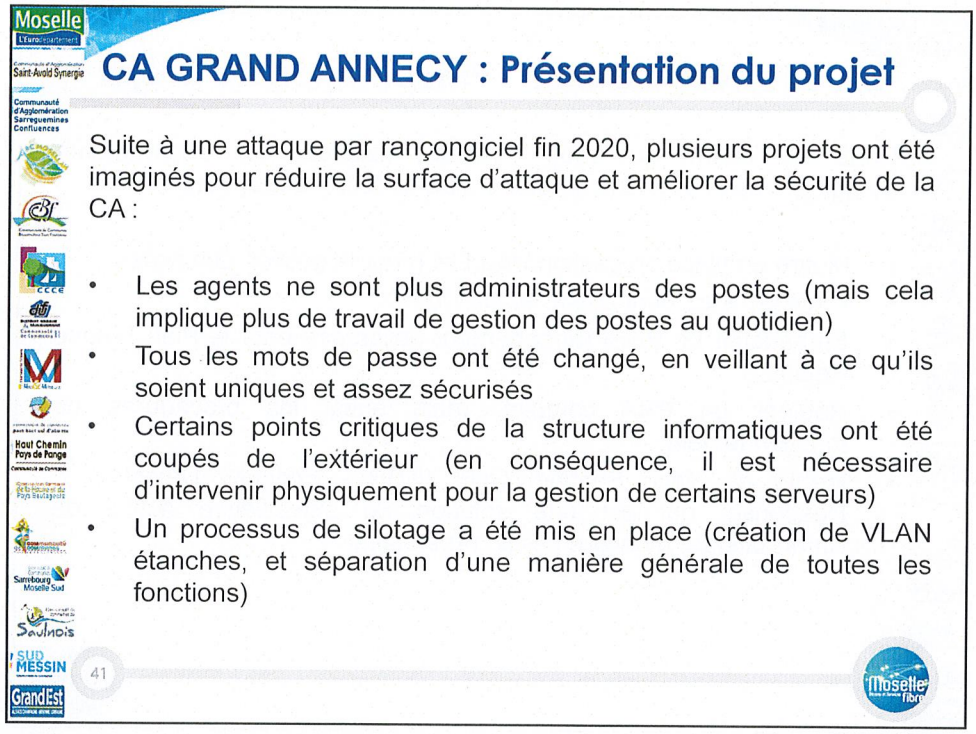
Périmètre d'action / membre : 34 communes, dont 20 communes de moins de 2 000 habitants et une ville-centre de plus de 130 000 habitants.

Nombre d'agents : 1200

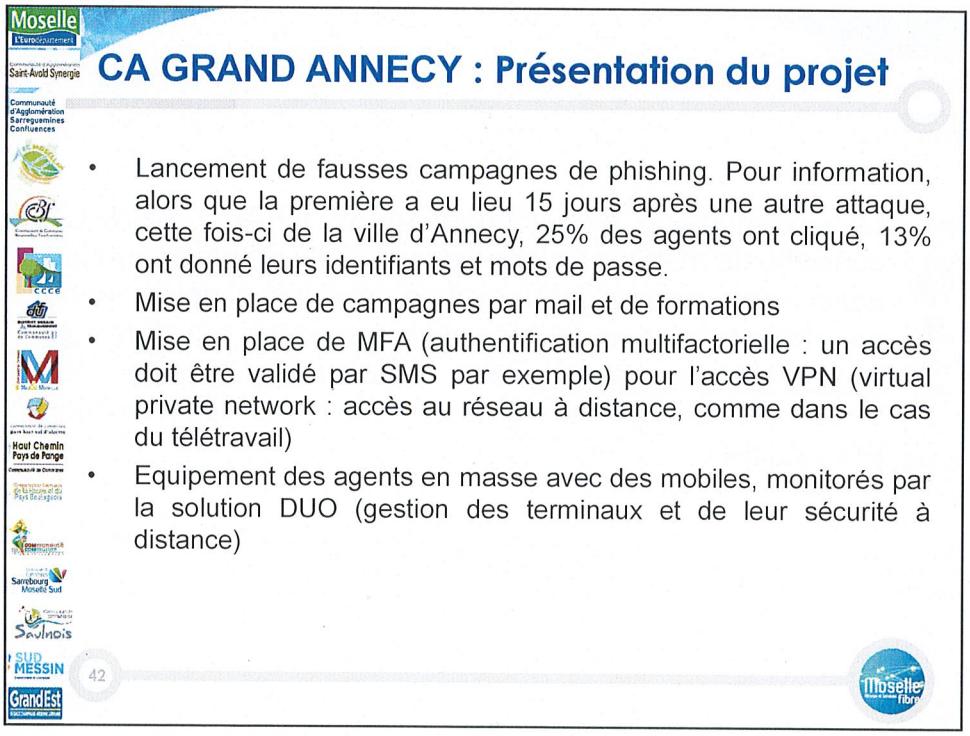
Il est à noter qu'il n'y pas de mutualisation informatique avec les communes de la CA. L'entretien ne concernait que des projets internes à la Communauté d'Agglomération.

40

40


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
Saulnois
SUD MESSIN
GrandEst
CA GRAND ANNECY : Présentation du projet
Suite à une attaque par rançongiciel fin 2020, plusieurs projets ont été imaginés pour réduire la surface d'attaque et améliorer la sécurité de la CA :
• Les agents ne sont plus administrateurs des postes (mais cela implique plus de travail de gestion des postes au quotidien)
• Tous les mots de passe ont été changé, en veillant à ce qu'ils soient uniques et assez sécurisés
• Certains points critiques de la structure informatiques ont été coupés de l'extérieur (en conséquence, il est nécessaire d'intervenir physiquement pour la gestion de certains serveurs)
• Un processus de silotage a été mis en place (création de VLAN étanches, et séparation d'une manière générale de toutes les fonctions)
41
Moselle Fibre

41


Moselle
L'Eurodépartement
Saint-Avold Synergie
Communauté d'Agglomération Sarreguemines Confluences
Haut Chemin Pays de Pange
Sarrebourg Moselle Sud
Saulnois
SUD MESSIN
GrandEst
CA GRAND ANNECY : Présentation du projet
• Lancement de fausses campagnes de phishing. Pour information, alors que la première a eu lieu 15 jours après une autre attaque, cette fois-ci de la ville d'Annecy, 25% des agents ont cliqué, 13% ont donné leurs identifiants et mots de passe.
• Mise en place de campagnes par mail et de formations
• Mise en place de MFA (authentification multifactorielle : un accès doit être validé par SMS par exemple) pour l'accès VPN (virtual private network : accès au réseau à distance, comme dans le cas du télétravail)
• Equipement des agents en masse avec des mobiles, monitorés par la solution DUO (gestion des terminaux et de leur sécurité à distance)
42
Moselle Fibre

42

CA GRAND ANNECY : Présentation du projet

Dans le cadre du Plan France Relance, la Communauté d'Agglomération a obtenu 90 000 € d'aides (2021-2022) pour :

- Mettre en place un bastion WALLIX (pour la gestion des accès)
- Protéger leurs données avec NETWRIX
- Embaucher un RSSI (engagement obligatoire pour le Plan France Relance)
- Rédiger un PRA complet, mais aussi les procédures de fonctionnement
- Mettre en place Sentinel ONE (EDR - Endpoint Detection & Response, qui est une solution de surveillance active de l'informatique) monitoré par un prestataire

43

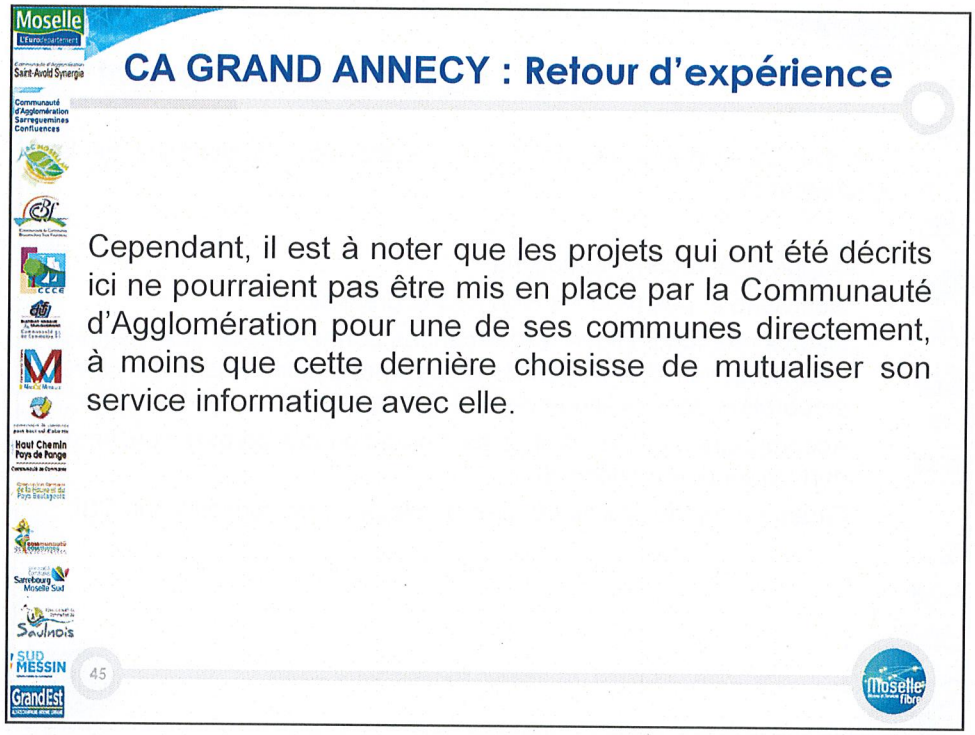
43

CA GRAND ANNECY : Retour d'expérience

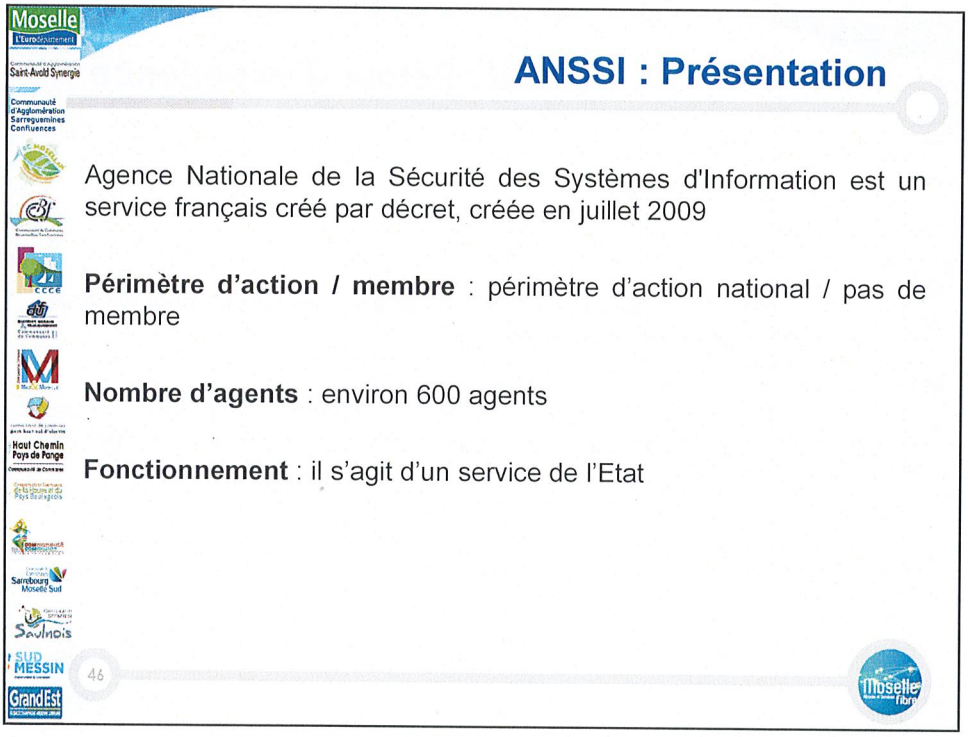
La Communauté d'Agglomération du GRAND ANNECY conseille de mettre en place des solutions de protection par anticipation, en soulignant qu'il ne s'agit pas simplement de projets ponctuels, mais bien d'un processus qui **doit être renouvelé en continu** car l'amélioration globale des protections entraine systématiquement une sophistication des attaques.

44

44


CA GRAND ANNECY : Retour d'expérience
Cependant, il est à noter que les projets qui ont été décrits ici ne pourraient pas être mis en place par la Communauté d'Agglomération pour une de ses communes directement, à moins que cette dernière choisisse de mutualiser son service informatique avec elle.
45

45


ANSSI : Présentation
Agence Nationale de la Sécurité des Systèmes d'Information est un service français créé par décret, créée en juillet 2009
Périmètre d'action / membre : périmètre d'action national / pas de membre
Nombre d'agents : environ 600 agents
Fonctionnement : il s'agit d'un service de l'Etat
46

46

ANSSI : Présentation du projet

L'ANSSI est porteuse de nombreux projets dans le domaine de la cybersécurité :

- Rapports et recommandations ;
- Qualification des produits, services et prestations ;
- Guides méthodologique recommandés pour l'Analyse des Risques, l'homologation des dispositifs et des protections mises en place, élaboration de la politique de sécurité des systèmes d'information ;
- Accompagnement, conseil et sensibilisation des acteurs concernés dans leurs démarches SSI ;
- Financement de projets de mise en place ou de consolidation SSI.

47

47

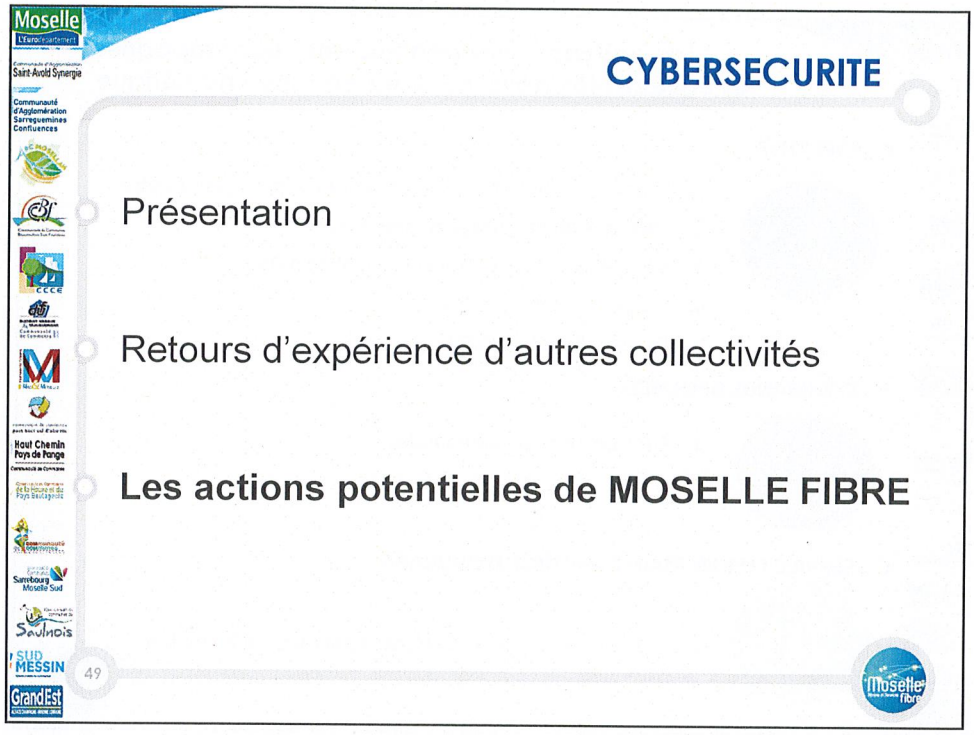
ANSSI : Retour d'expérience

L'ANSSI est, de par sa fonction même, une entité littéralement centrale dans la thématique de la cybersécurité.

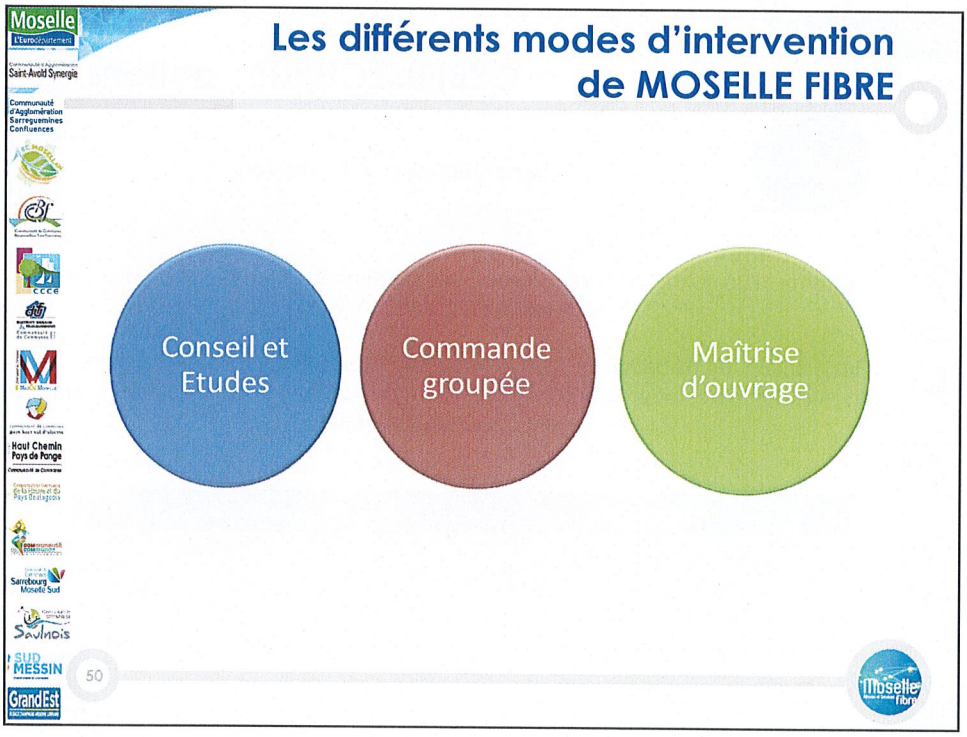
Il est donc primordial que l'action de MOSELLE FIBRE puisse s'interfacer avec les projets nationaux déjà en place, soit en les complétant, soit en accompagnant les collectivités à y faire appel.

48

48


Moselle
L'Eurodépartement
CYBERSECURITE
Présentation
Retours d'expérience d'autres collectivités
Les actions potentielles de MOSELLE FIBRE
49

49


Moselle
L'Eurodépartement
Les différents modes d'intervention de MOSELLE FIBRE
Conseil et Etudes
Commande groupée
Maîtrise d'ouvrage
50

50

Les actions envisageables pour accompagner les collectivités dans leur transformation numérique

A. EXPERTISE

Conseil et Etudes

1. Sensibilisation et formation à destination du grand public
2. Information et partage d'expérience
3. Réalisation d'audit de sécurité informatique
4. Mutualisation d'un RSSI
5. Bureau d'étude / AMO

B. COMMANDE GROUPEE

Groupement Commandes

1. Groupement de commandes

C. SERVICE CLEF EN MAIN / MAITRISE D'OUVRAGE

Maîtrise d'ouvrage

1. Surveillance de la sécurité des systèmes d'information

51

51

CYBERSECURITE : actions

Conseil et Etudes

1. Sensibilisation et formation

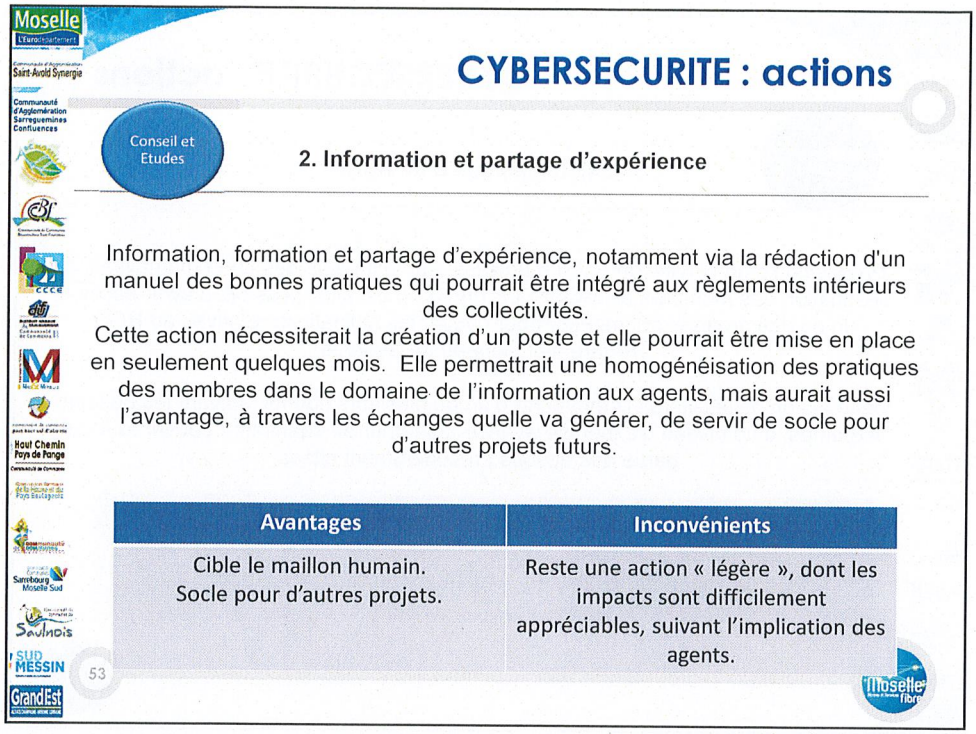
Intégration d'un volet complet de cybersécurité dans les formations médiation à destination du grand public.

Cette action, ne nécessitant pas de recrutement ni d'investissement, pourrait être mise en place pour la prochaine session de formation des médiateurs, via la création d'un atelier dédié.

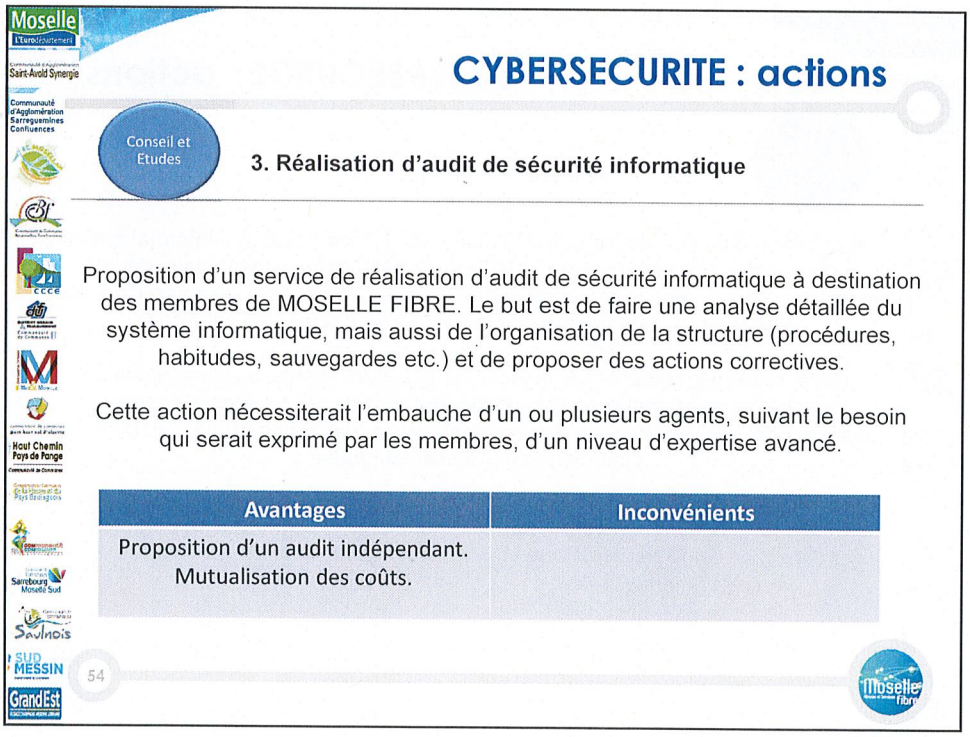
Avantages	Inconvénients
Facilité de mise en œuvre. Il y a déjà une introduction sur la sécurité informatique dans les formations actuelles.	

52

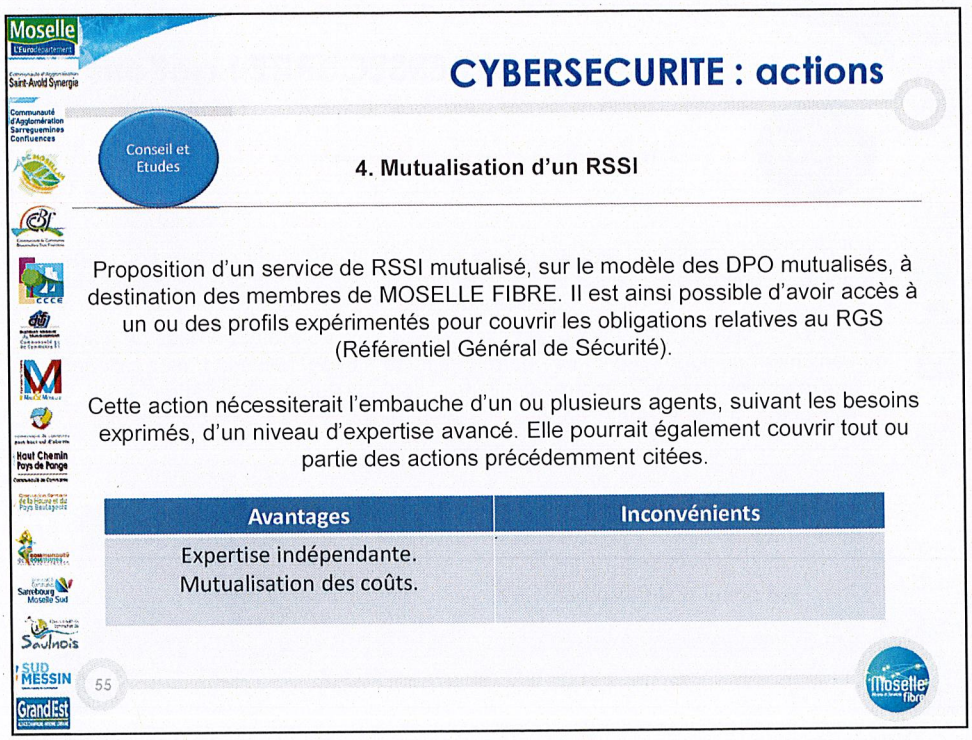
52


CYBERSECURITE : actions
Conseil et Etudes
2. Information et partage d'expérience
Information, formation et partage d'expérience, notamment via la rédaction d'un manuel des bonnes pratiques qui pourrait être intégré aux règlements intérieurs des collectivités.
Cette action nécessiterait la création d'un poste et elle pourrait être mise en place en seulement quelques mois. Elle permettrait une homogénéisation des pratiques des membres dans le domaine de l'information aux agents, mais aurait aussi l'avantage, à travers les échanges quelle va générer, de servir de socle pour d'autres projets futurs.
Avantages
Inconvénients
Cible le maillon humain.
Socle pour d'autres projets.
Reste une action « légère », dont les impacts sont difficilement appréciables, suivant l'implication des agents.
53

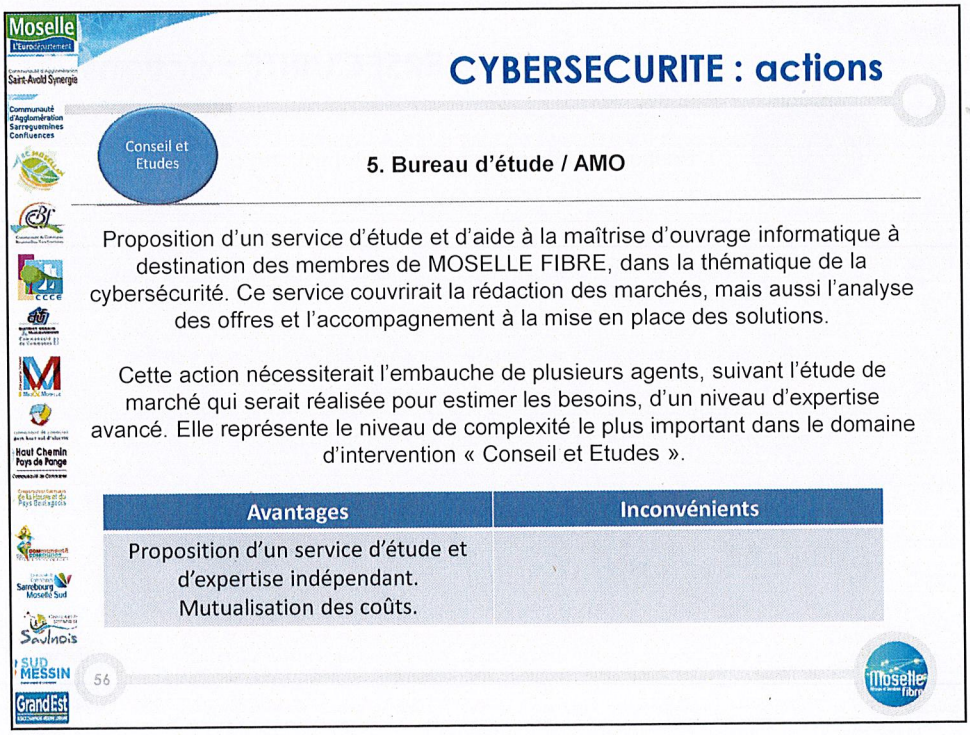
53


CYBERSECURITE : actions
Conseil et Etudes
3. Réalisation d'audit de sécurité informatique
Proposition d'un service de réalisation d'audit de sécurité informatique à destination des membres de MOSELLE FIBRE. Le but est de faire une analyse détaillée du système informatique, mais aussi de l'organisation de la structure (procédures, habitudes, sauvegardes etc.) et de proposer des actions correctives.
Cette action nécessiterait l'embauche d'un ou plusieurs agents, suivant le besoin qui serait exprimé par les membres, d'un niveau d'expertise avancé.
Avantages
Inconvénients
Proposition d'un audit indépendant.
Mutualisation des coûts.
54

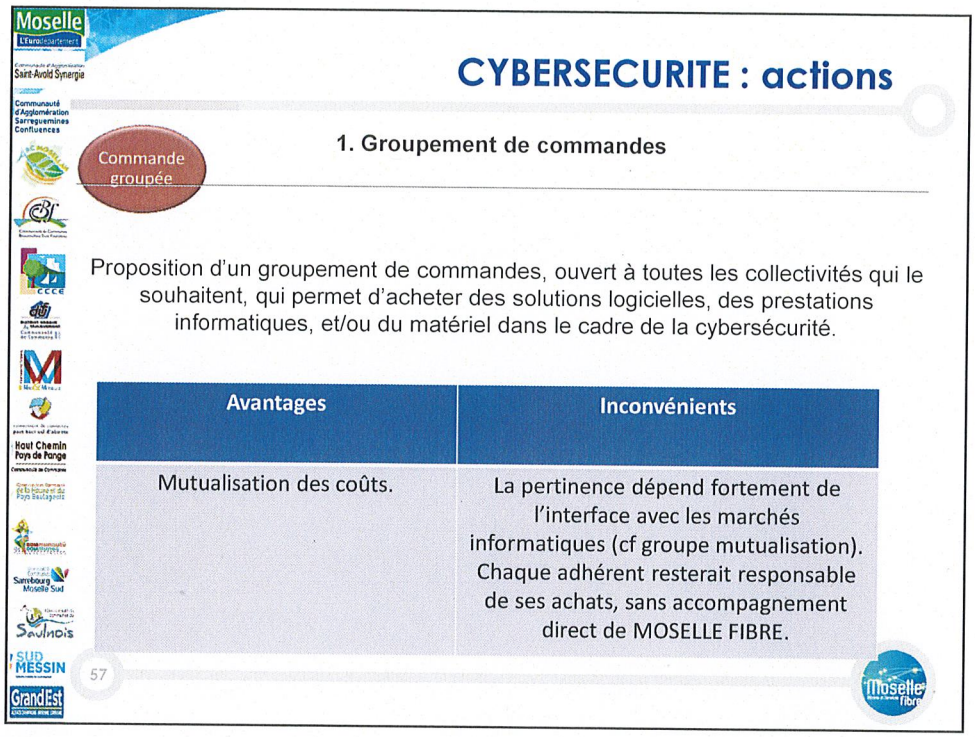
54


CYBERSECURITE : actions
Conseil et Etudes
4. Mutualisation d'un RSSI
Proposition d'un service de RSSI mutualisé, sur le modèle des DPO mutualisés, à destination des membres de MOSELLE FIBRE. Il est ainsi possible d'avoir accès à un ou des profils expérimentés pour couvrir les obligations relatives au RGS (Référentiel Général de Sécurité).
Cette action nécessiterait l'embauche d'un ou plusieurs agents, suivant les besoins exprimés, d'un niveau d'expertise avancé. Elle pourrait également couvrir tout ou partie des actions précédemment citées.
Avantages
Inconvénients
Expertise indépendante.
Mutualisation des coûts.
55

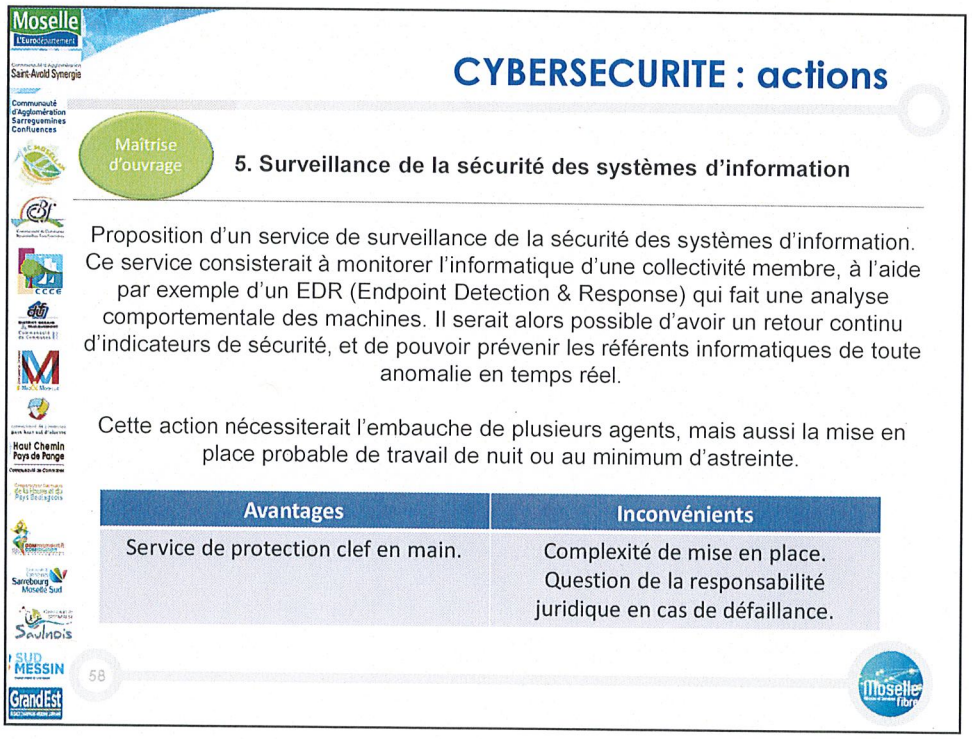
55


CYBERSECURITE : actions
Conseil et Etudes
5. Bureau d'étude / AMO
Proposition d'un service d'étude et d'aide à la maîtrise d'ouvrage informatique à destination des membres de MOSELLE FIBRE, dans la thématique de la cybersécurité. Ce service couvrirait la rédaction des marchés, mais aussi l'analyse des offres et l'accompagnement à la mise en place des solutions.
Cette action nécessiterait l'embauche de plusieurs agents, suivant l'étude de marché qui serait réalisée pour estimer les besoins, d'un niveau d'expertise avancé. Elle représente le niveau de complexité le plus important dans le domaine d'intervention « Conseil et Etudes ».
Avantages
Inconvénients
Proposition d'un service d'étude et d'expertise indépendant.
Mutualisation des coûts.
56

56


CYBERSECURITE : actions
Commande groupée
1. Groupement de commandes
Proposition d'un groupement de commandes, ouvert à toutes les collectivités qui le souhaitent, qui permet d'acheter des solutions logicielles, des prestations informatiques, et/ou du matériel dans le cadre de la cybersécurité.
Avantages
Inconvénients
Mutualisation des coûts.
La pertinence dépend fortement de l'interface avec les marchés informatiques (cf groupe mutualisation). Chaque adhérent resterait responsable de ses achats, sans accompagnement direct de MOSELLE FIBRE.
57

57


CYBERSECURITE : actions
Maîtrise d'ouvrage
5. Surveillance de la sécurité des systèmes d'information
Proposition d'un service de surveillance de la sécurité des systèmes d'information. Ce service consisterait à monitorer l'informatique d'une collectivité membre, à l'aide par exemple d'un EDR (Endpoint Detection & Response) qui fait une analyse comportementale des machines. Il serait alors possible d'avoir un retour continu d'indicateurs de sécurité, et de pouvoir prévenir les référents informatiques de toute anomalie en temps réel.
Cette action nécessiterait l'embauche de plusieurs agents, mais aussi la mise en place probable de travail de nuit ou au minimum d'astreinte.
Avantages
Inconvénients
Service de protection clef en main.
Complexité de mise en place.
Question de la responsabilité juridique en cas de défaillance.
58

58