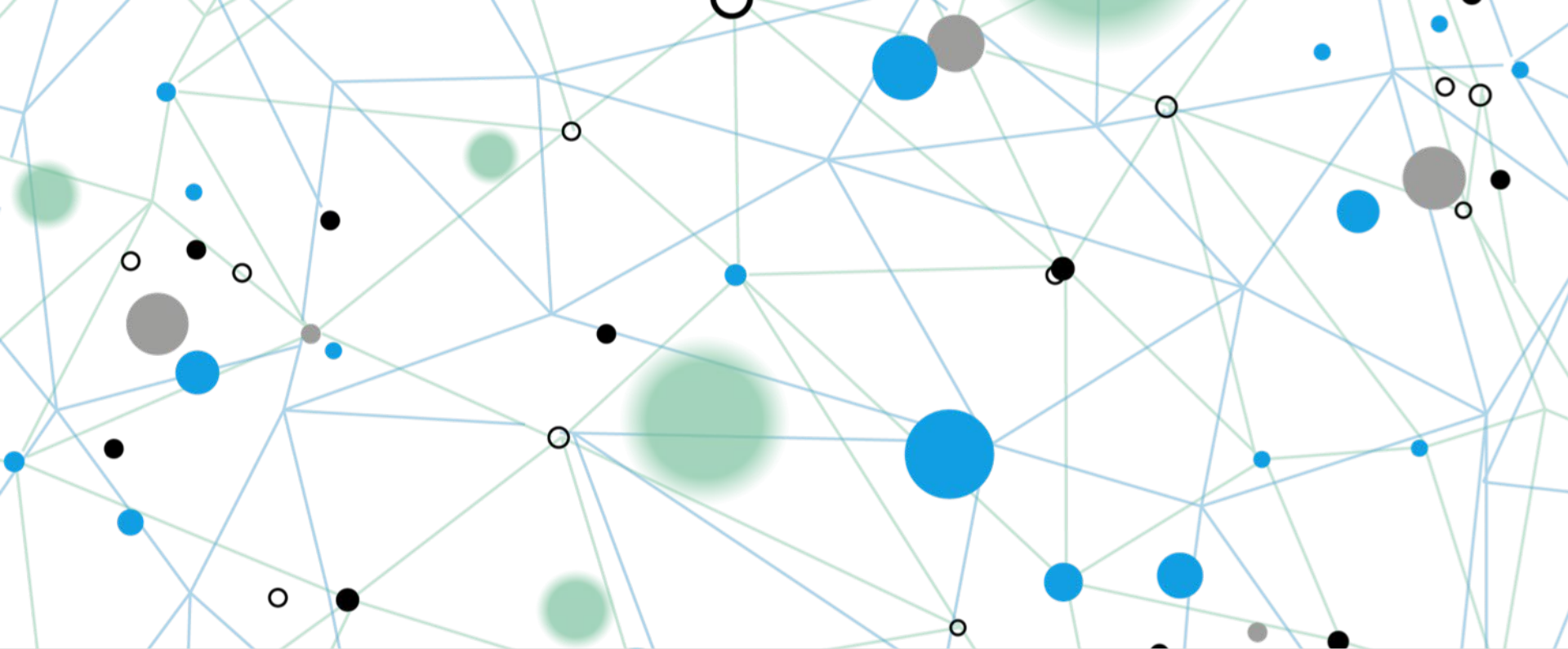




SEINE-ET-MARNE
NUMÉRIQUE



TRIP Avicca

Table ronde - Cybersécurité 12 mai 2021

Contexte SMN



SEINE-ET-MARNE
NUMÉRIQUE

Un SI pour qui, pour quoi ?

Une « petite » équipe de 15 personnes

Une activité d'aménagement numérique sur 50% du territoire d'Ile-de-France :

- **RIP 1G FttO et THD Radio**
- **RIP 2G FttE/FttH affermo-concessif**
- **Exploitation parc PRM MeD en régie**

Le SI en bref

Fonction SI portée par la DAF :

- **Une assistante pour traitement des tâches courantes**
- **Une directrice pour pilotage et supervision**

Une architecture repensée en 2018 :

- **Serveur en propre hébergé en salle SI du département - baie dédiée sans adhérence**
- **Lien FON entre le syndicat et le site d'hébergement**
- **Téléphonie en IP Centrex**
- **Accès Internet FTTO**

Une infogérance via marché de service

Contexte SMN



SEINE-ET-MARNE
NUMÉRIQUE

Des mesures de sécurité préexistantes et en place

- **Anti-virus sur chaque poste de travail (SOPHOS)**
- **Pare-feu entre la téléphonie fixe et l'accès internet**
- **Politique de blocage de l'accès à certains sites internet**
- **Mots de passe utilisateurs à 8 caractères + caractères spéciaux**
- **Processus de renouvellement automatique des mots de passe utilisateurs**
- **Confidentialité des mots de passe administrateurs**
- **Logiciel anti-spam (MIB)**
- **Sauvegarde avec réplication (VEEAM Backup)**
- **Réplication des serveurs centraux sur le site du syndicat via la solution VMware**
- **Accès VPN sécurisé avec mot de passe individuel**

Faits

Prise de poste le lundi 8 février 2021 matin : les agents constatent l'impossibilité d'accéder aux fichiers et dossiers enregistrés sur les serveurs. L'ensemble est crypté par une extension « .e344p8xk »

 Classeur1.xlsx.e344p8xk	06/02/2021 20:22	Fichier E344P8XK	12 Ko
 signature_élec_SMN77_JDC.jpg.e344p8xk	06/02/2021 20:22	Fichier E344P8XK	28 Ko
 SMN petit.png.e344p8xk	06/02/2021 20:22	Fichier E344P8XK	26 Ko

9h48 : ouverture d'un ticket auprès du support technique informatique de l'infogérant

10h00 à 13h00 : prise de main à distance sur postes et serveurs. Les documents impactés se trouvent sur la machine VM-DATA-01 cryptée depuis samedi soir à 20h22

Autre constat : la sauvegarde n'est plus fonctionnelle depuis le 23/01

13h00 à 15h00 : plan d'action - vérification des LOG sur le Firewall - coupure de tous les serveurs « utilisateurs » - création d'un réseau isolé BAC A SABLE pour identifier la source du cryptolocker. En parallèle, restauration de la VM-DATA-01 à partir de la dernière sauvegarde du 23/01/21.

Faits - suite



SEINE-ET-MARNE
NUMÉRIQUE

**09/02/2021 : restauration de la VM terminée à 100%. Pas de nouveau cryptage
mise en place d'une supervision renforcée de la solution Veeam Backup**

10/02/2021 : l'infrastructure est de nouveau opérationnelle

11/02/2021 : divers problèmes sont constatés notamment par les utilisateurs en accès VPN

12/02/2021 : finalisation de la reconstruction de la VM-DATA-01

12/02/2021 : l'infrastructure est opérationnelle

**En sus, déclaration à l'assureur et rejet car pas d'assurance cybersécurité spécifique,
déclaration à la CNIL, plainte au commissariat (classement sans suite depuis lors)**

Informations aux agents tout au long du process

Mesures



SEINE-ET-MARNE
NUMÉRIQUE

1 - Mesures immédiates

- **Modification de toutes les extensions VPN (suppression du .local / accès VPN unifiés avec le compte Active Directory)**
- **Modification de tous les mots de passe d'accès VPN**
- **Accès direct des agents comptables en télétravail au logiciel Finances**
- **Doublement des emails de supervision de sauvegarde à deux agents de la DAF**
- **Audit de l'ensemble des anti-virus**
- **Sensibilisation des agents aux gestes à respecter (mise en ligne documentation ANSSI, comment bâtir un mot de passe complexe, etc.)**

2 - Mesures en cours

- **Suppression de la possibilité pour chaque agent d'être administrateur de son poste (même en raison du logiciel téléphonie fixe ou métier)**
- **Renforcement de l'anti-virus**
- **Étude sur le choix d'une sauvegarde des données sur bande (règle du 3-2-1)**
- **Souscription d'une assurance cybersécurité**

Impacts



SEINE-ET-MARNE
NUMÉRIQUE

Minimes en termes de perturbations du travail

Les données sensibles (ex. : RH) cryptées n'ont pas été communiquées à l'extérieur. Les effets ont donc été limités.

Mais, double sauvegarde inopérante depuis le 23/01/2021 et perte de l'ensemble des documents produits ou modifiés sur le réseau jusqu'au 06/02/2021.

Inventaire de ces documents finalisé = perte de l'ensemble des courriers entrants/sortants, bons de commande émis, mises à jour de tableaux de suivi (conventions, marchés publics, suivi financier, indicateurs), permissions de voirie, ordres de service et procès-verbaux, des calendriers et ordres du jour et certains archivages.

Le cryptolocker n'ayant pu être trouvé, le risque d'une nouvelle cyberattaque demeure réel.

Enseignements



SEINE-ET-MARNE
NUMÉRIQUE

- **Établir une revue de sécurité du SI régulière (check list)**
- **Prévoir deux à trois sauvegardes des données**
- **Vérifier les modes de fonctionnement des sauvegardes**
- **Vérifier que les VM sont suffisamment dimensionnées pour permettre qu'en cas d'attaque, il n'y ait pas besoin de les « écraser » pour rendre le service à nouveau opérationnel**
- **Recourir à une assurance cybersécurité**
- **Sensibiliser les agents à la sécurité informatique en continu**



SEINE-ET-MARNE
NUMÉRIQUE

Merci de votre attention

Contact : Julie DULAC
Directrice administrative et financière
julie.dulac@seineetmarnenumerique.fr
01 64 10 66 13