

COMpte-RENDU ATELIER CYBERSÉCURITÉ ET COLLECTIVITÉS TERRITORIALES

Animateur



Raymond VALL, *Sénateur du Gers*

Participants



Thibault CHENEVIÈRE, *Adjoint au numérique à la Mairie de Pau*



Pierre GACIC, *Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)*



Colonel Philippe BAUDOIN, *DGGN*



El-Yamani HAMED, *ENGIE INEO DEFENSE*



Thibault CHENEVIERE
Adjoint au numérique à la
Mairie de Pau

Thibault Cheneviere dans le rôle de l'orateur principal a posé les principaux axes de réflexions : il s'agit en premier lieu de faire un constat de diversité. En effet, les collectivités territoriales sont de tailles, de moyens, et d'organisations très différents. Dans la même veine, il est à noter les différents degrés de numérisation des Mairies. Est aussi abordée la stratification des collectivités et la multiplicité des acteurs présents (agents de mairie, direction des services, etc....).

« L'aspect sécurité n'est pas pris en compte dans les démarches de numérisation, qui ne sont orientées que vers une recherche de présence et de représentation numérique. »

Les acteurs notent une prise de conscience autrement supérieure dans le privé qui amorce un virage numérique beaucoup plus fort.



Colonel Philippe BAUDOIN
DGGN

Dans la conjoncture post-attentats, la situation se dégrade, les actions de type piratage de sites Internet se multiplient. L'expérience du Colonel permet de mettre en lumière un certain amateurisme de la part des collectivités, qui fonctionnent assez souvent sans profondeur et sans suivi sur ces dossiers. Le site de la mairie peut rapidement tomber en déshérence après un changement de majorité, etc.... La chaîne numérique semble fragile.

D'autre part, l'aspect sécurité n'est pas pris en compte dans les démarches de numérisation, qui ne sont orientées que vers une recherche de présence et de représentation numérique.

Or, les collectivités sont vulnérables aux risques : elles détiennent souvent, sans le savoir, des informations qui peuvent être très sensibles parmi lesquels les cadastres, la liste des états civils... L'enjeu sécuritaire sur ces thèmes est très forts.

Sont abordés les vecteurs de risques :

- Emails piégés : relèvent d'un grave problème de sensibilisation des agents.
- Intrusions diverses : souvent à l'insu des acteurs.

- Rançon-giciels : i.e. rançon contre déblocable total ou partiel, rançon à l'information ou au cryptage.

« Les collectivités sont vulnérables aux risques : elles détiennent souvent, sans le savoir, des informations qui peuvent être très sensibles. »

- Faux virements (là aussi on traite avec de la méconnaissance des règles de sécurités et de bonnes pratiques).

Il est à rappeler que 95% des attaques ont pour but l'escroquerie et 5% l'attaque réelle.

Pierre GACIC
Agence Nationale de Sécurité des
Systèmes d'Information (ANSSI)



Expose le dispositif de l'ANSSI à destination des collectivités. C'est une organisation jeune, encore en plein déploiement. L'ANSSI note la différence entre les TPE et PME, qui ne détiennent pas d'informations sensibles, contrairement aux petites collectivités qui sont alors une cible de choix. La problématique est alors de toucher et de sensibiliser des acteurs locaux souvent occupés et non acculturés à ces thèmes sécuritaires, auxquels ils n'attachent que peu d'intérêt.

EI-Yamani HAMED
ENGIE INEO DEFENSE



Le problème de l'identification se pose autant pour la menace que pour l'information sensible. Nous présente les différentes motivations récurrentes des attaquants qui sont : idéologiques, anarchiques, financières... Mais surtout de recherche de capacité !

« La problématique est de toucher et de sensibiliser des acteurs locaux souvent occupés et non acculturés à ces thèmes sécuritaires, auxquels ils n'attachent que peu d'intérêt. »

Certaines attaques ont vocation à permettre la mise en place d'une attaque de plus grande ampleur vers un acteur plus important. Les collectivités et leurs outils connectés pouvant n'être que de simples relais dans ce cas. Dans ce contexte les attaquants sont peu identifiables et

représentent un risque très fort si elles ne sont pas détectées comme des signaux faibles.
La question du marché de l'information privée est aussi une grande menace selon.

Pierre Gacic rappelle la loi NOTRe (la loi portant Nouvelle Organisation Territoriale de la République) du 7 août 2015, sur le développement des compétences des Régions, qui les exposent encore plus, sans mettre en place de plan de protection. La problématique est alors celle du contact et de l'accompagnement.

Pierre GACIC
ANSSI



« L'accompagnement passe par le référent sûreté en Région. Il est le lien entre l'État et les acteurs locaux, et a la capacité de l'évaluation de la sûreté, ainsi que d'orienter le Maire vers le bon acteur. »



Colonel Philippe BAUDOIN
DGGN

C'est dans ce cadre que l'ANSSI a élaboré et mis en place son dispositif de coordinateur dans chaque région. C'est lors de grands événements que les acteurs peuvent être approchés. L'objectif de l'ANSSI étant de faire gagner en maturité les acteurs publics.

L'ANSSI est orientée vers l'État. La DGSi s'oriente davantage vers les acteurs privés plutôt que vers les collectivités territoriales. L'accompagnement passe par le référent sûreté en Région présent au sein des brigades : ce dernier est le lien entre l'État et les acteurs locaux. C'est lui qui a la capacité de l'évaluation de la sûreté, ainsi que d'orienter le Maire vers le bon acteur.

EI-Yamani HAMED
ENGIE INEO DEFENSE



« La cybersécurité est avant tout une posture humaine et l'on revient au fait qu'il faut une prise de conscience de l'ensemble des acteurs et des personnels. »

La cybersécurité est avant tout une posture humaine et l'on revient au fait qu'il faut une prise de conscience de l'ensemble des acteurs et des personnels. Pour aborder cette cybersécurité au sein des collectivités territoriales, il faut aussi prendre en compte la réglementation, la CNIL, les préconisations de l'ANSSI... L'importance d'inclure dans les appels d'offres la notion de sécurité doit aussi faire partie de cette prise de conscience.

C'est le principe de la recherche qui doit aussi ici être abordé : en effet, l'objectif commun de la DGSi et de l'ANSSI sur ces sujets n'est pas le dépôt de plaintes, mais l'alerte, qui permet l'identification et la compréhension des évolutions des techniques et des moyens dans les attaques.



CE QU'IL FAUT RETENIR

- ◆ L'aspect sécurité doit être pris en compte dans les démarches de numérisation.
- ◆ Les collectivités sont vulnérables aux risques : elles détiennent sans le savoir des informations qui peuvent être très sensibles.
- ◆ La cybersécurité est avant tout une posture humaine et l'on revient au fait qu'il faut une prise de conscience de l'ensemble des acteurs et des personnels.
- ◆ L'accompagnement passe par le référent sûreté en Région. Il est le lien entre l'État et les acteurs locaux, et a la capacité de l'évaluation de la sûreté, ainsi que d'orienter le Maire vers le bon acteur.