REVUE DE PRESSE/THE CONVERSATION

Cybersécurité : le défi de la formation des dirigeants publics

Les informations et les données qui tentent d'évaluer la prise en compte par les dirigeants de collectivités territoriales de la Sécurité de leurs propres Systèmes d'Information (SSI) sont assez rares en général et restent quasiment inexistantes en France. Une nouvelle étude, récemment publiée, expose, à nouveau, un niveau de prise en compte qui reste globalement insuffisant. Elle pointe un niveau de vulnérabilité qu'il convient de prendre au sérieux. [...] Lire la suite

Il est pourtant manifeste, en ces temps troublés, que cette sécurisation des SI des collectivités territoriales – et des bases de données sensibles de type public et para public qu'ils renferment – constitue un impératif stratégique tout à fait majeur. Cet impératif dépasse largement le simple cadre local et territorial notamment au regard de l'augmentation constante des cyberattaques et des cybermenaces contre des collectivités, y compris de taille modeste, voire très modeste, depuis le début des crises sanitaires et sécuritaires que nous traversons depuis 2020. Selon un rapport du cabinet Asterès, les organisations publiques ont subi 37 000 cyberattaques réussies en 2022. La moitié de celles employant plus de 250 salariés sont concernées mais plus d'un quart (27 %) demeurent en deçà de 250 salariés.

Un sentiment de maîtrise en trompe-l'œil

Pour tenter de combler ce déficit de sécurité, il nous a semblé que trois fondements théoriques issus des sciences de gestion et du management public étaient à mobiliser. Le premier repose sur travaux liés à l'adoption et à l'appropriation des outils numériques en mode TOE. Ceux-ci s'intéressent à ce qui relève de la technologie, de l'organisation ou de l'environnement dans les prises de décision en matière de cybersécurité. Le second s'intéresse aux travaux sur les risques numériques en organisation publique et le décalage entre les dangers potentiels et la maîtrise que pensent en avoir les agents. Le troisième pilier est lié aux travaux sur la prévention des cyberattaques publiés par Rémy Février.

Pour aller plus loin qu'un seul cadrage théorique et aborder les aspects empiriques propres au terrain, nous avons mobilisé 67 dirigeants de collectivités qui, toutes, ont moins de 3 500 habitants et sont situées en métropole. Les questionnaires qu'ils nous ont retournés ont été traités statistiquement à la fois de façon descriptive et par classification hiérarchique.

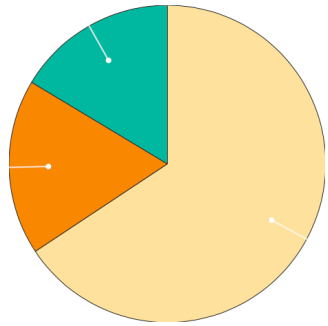
Il s'agissait de s'attaquer à la question du « pourquoi » de cette vulnérabilité en décryptant les freins retardant le déploiement d'une véritable politique de sécurisation des SI des collectivités territoriales.

Le premier est collectif et réside dans le vocabulaire employé qui doit rester accessible à tous. Il convient ainsi de ne pas trop « techniciser » les menaces et d'appeler un chat un chat sans trop de jargon ni verbiage. Par exemple des termes basiques comme « mot de passe », « pièce jointe », « lien » ou « hameçonnage » ne doivent pas être snobés ! Les autres freins sont plus individuels et montrent certaines lacunes – non rédhibitoires – en matière de prise de conscience de la réalité des risques numériques par les décideurs territoriaux.

À titre d'exemple, nous avons pu mettre en lumière trois types de profils de dirigeants que nous avons qualifiés de « 3P »

16 % de prudents seulement

On retrouve en premier lieu les « **Pratiques** », qui représentent 65,7 % de l'effectif total. Cette classe correspond aux dirigeants utilisant normalement les technologies de l'information et de la communication (TIC), relativement bien informés à propos des risques liés à l'utilisation d'un SI. Cependant, ces derniers ne sont que faiblement conscients de la nécessité de protéger leurs données numériques et encore moins de la réglementation afférente. La majorité de ce premier type de profil représente des individus issus de communes de moins de 3 500 habitants (56 %) et provient de directions générales (40 %).



Les questionnaires ont été soumis à 67 dirigeants de collectivités qui, toutes, ont moins de 3 500 habitants.
Graphique: The Conversation France CC • Source: Auteurs • Insérer • Créé avec Datawrapper

Les « **Perplexes** » regroupent, eux, 17,9 % de l'effectif total. Il s'agit de dirigeants cumulant un certain nombre de lacunes en matière de prise en compte de la sécurité de leur SI respectif. Ils restent très peu utilisateurs des TIC, pas du tout informés sur les menaces liées au SI et peu sensibles aux questions de sécurité. Les individus de ce groupe sont pour 66 % des élus, issus en majorité de communes de moins de 1 000 habitants (91 %) et disposant en moyenne de trois fonctionnaires territoriaux.

Les « **Prudents** », enfin, 16,4 % de l'effectif total, sont les dirigeants les plus conscients de l'apport des SI et de leur nécessaire sécurisation. Ces individus ont un usage intensif des TIC (45 %), ils sont très bien informés sur les menaces liées au SI (72 %), bien organisés (81 %) et ont une relative conscience du caractère sensible des données traitées par le SI (72 %). Ce dernier type de profil vit en majorité dans des communes de plus de 1 000 habitants (63 %) et travaille dans des structures employant en moyenne 107 agents. Les cadres informatiques représentent une part importante de cette classe (40 %).

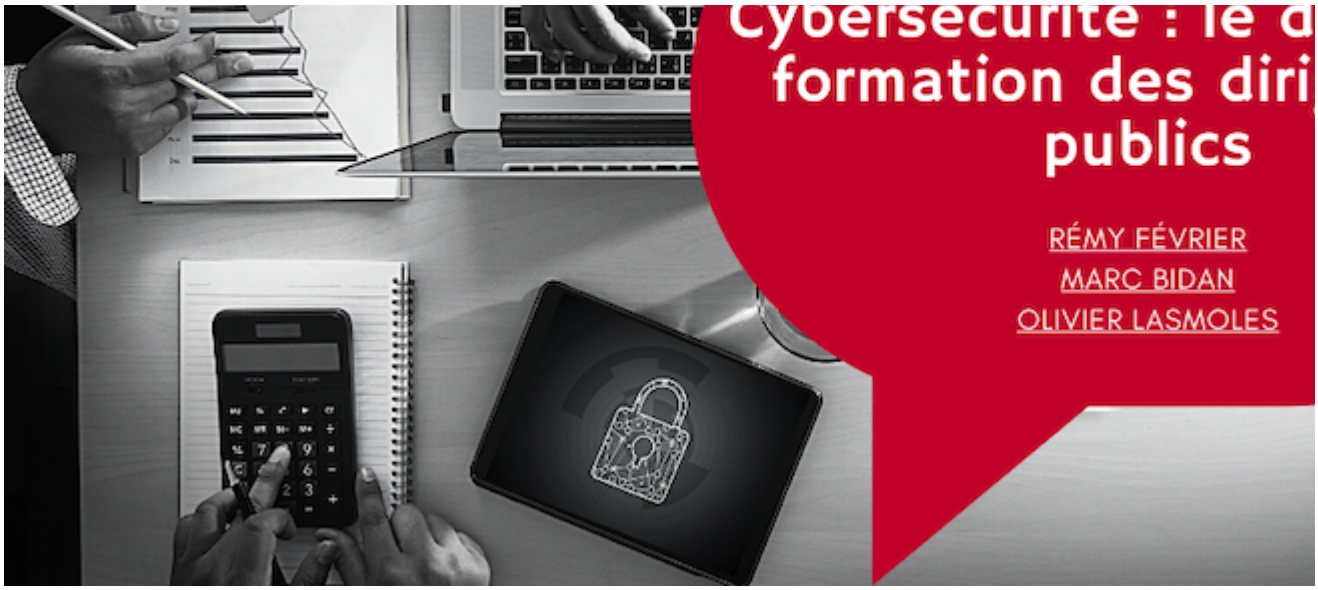
Quelques perspectives

Ces dernières années le niveau de formation et d'information des employés est certes monté mais pas forcément aussi vite que celui du risque d'être attaqué et fragilisé.

Il faut donc rester vigilant – la limite de ce type d'enquête est que les données collectées sont vite obsolètes – et prudent pour continuer à monter en puissance. Il ne faut en effet rien négliger pour mieux former et informer nos dirigeants – quelque soit leur parcours professionnel préalable (ingénieur, manageurs, employés, juristes, etc.) – à la fois sur l'information (nous sommes en effet vulnérables mais il est possible de déployer des solutions de confiance !) et sur la formation (nous pourrions ne plus, ne pas ou – restons humbles – moins l'être !) de façon à contribuer à l'opérationnalisation d'une démarche volontariste de sécurisation de nos SI.

Gardons enfin à l'esprit que des quatre composantes de nos systèmes d'information – réseaux, matériel, logiciel et personnel – il est bien évident que c'est la dernière qui doit faire l'objet de toute notre attention – via le déploiement de cyberréflexes – car d'une part c'est la "porte d'entrée" la plus fréquemment utilisée et d'autre part "l'intelligence artificielle générative va aider les cybercriminels à créer de nouveaux modèles ».

Source : The Conversation



5 décembre 2023

+ **Lire l'article sur The Conversation**

Les auteurs

Rémy Février

Maître de conférences HDR en Sciences de gestion et membre du laboratoire Équipe Sécurité & Défense - Renseignement, criminologie, crises, cybermenaces (ESDR3C) du Cnam.

+ **En savoir plus**

Marc Bidan

Professeur des Universités en Management des systèmes d'information - Nantes Université

Olivier Lasmoles

Associate Professor in Law - Skema, SKEMA Business School