Les ASSISES de la CYBERSÉCURITÉ 2023

Seine et Yvelines Numérique

L'innovation au service de tous

Document édité par
Seine-et-Yvelines Numérique
15 bis, avenue du Centre, 78280 Guyancourt

Conception éditoriale :
Seine-et-Yvelines Numérique

Comité de rédaction :
Laurent Rochette & Judith Thépot

Rédaction & conseil éditorial :
Corinne Martin-Rozès

Création & réalisation :
Tribu - MV Group

SOMMAIRE

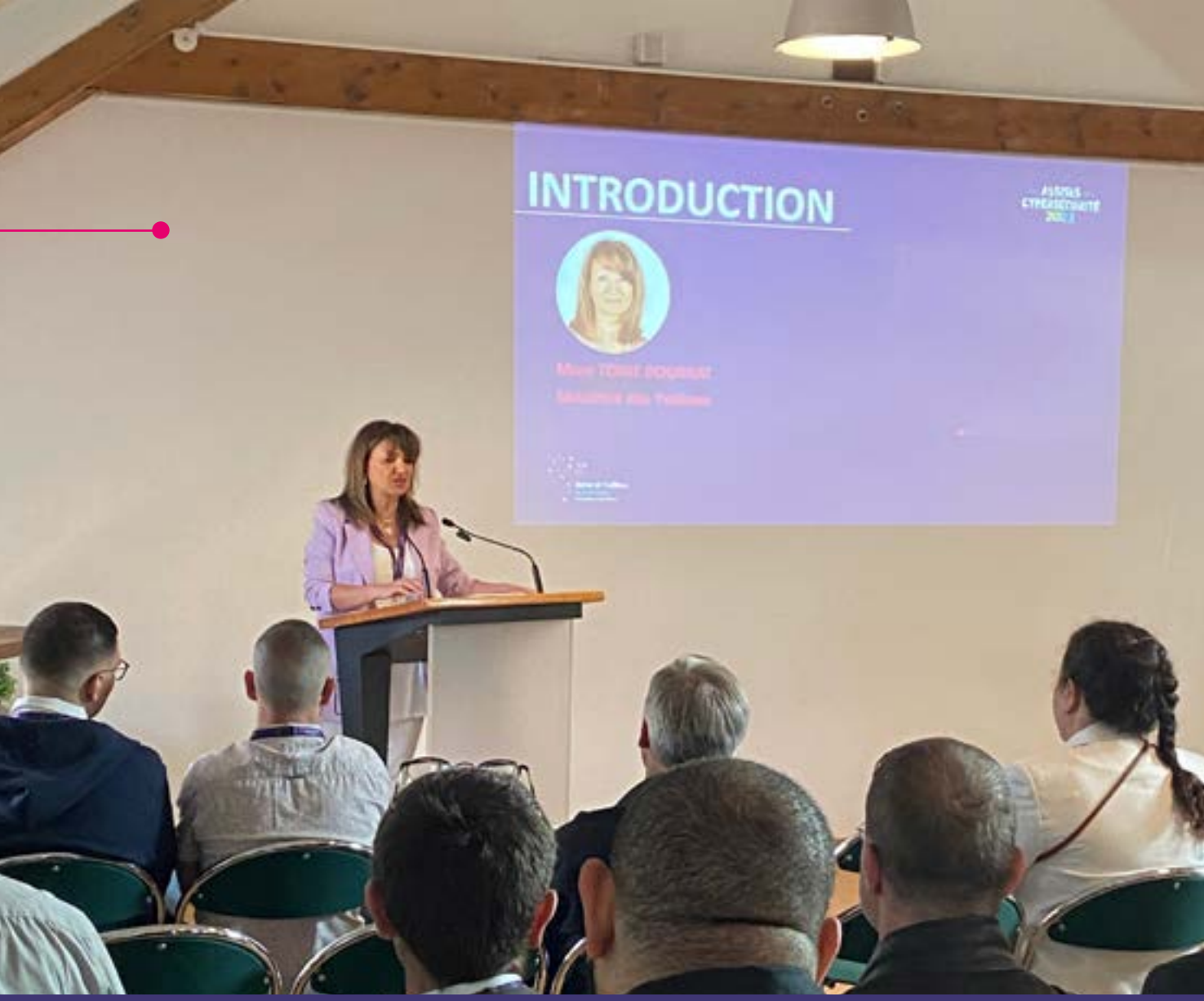
ÉDITORIAL

FORCE DOIT RESTER À LA LOI, Y COMPRIS DANS LE CYBERESPACE

Je suis très heureuse d'ouvrir ces Assises Cybersécurité, et je remercie Seine-et-Yvelines Numérique pour cette invitation. Un tel événement consacre l'engagement du Département des Yvelines et de son président, Pierre Bédier, en faveur d'un accompagnement des acteurs publics exposés, comme nous le sommes tous, aux défis d'internet.

Aujourd'hui, chacun de nos actes revêt une dimension numérique et le cyberespace est devenu une extension du domaine de la vie en société. Nous vivons à ce titre depuis deux décennies un bouleversement civilisationnel, un choc culturel et scientifique. Pour conserver sa souveraineté, l'homme doit recouvrer la maîtrise de son destin, y compris sur la toile. Or nous partageons tous, acteurs publics, une vocation : celle d'agir pour la collectivité, de protéger les entités et les êtres les plus vulnérables, en prônant une vision préventive et non plus seulement curative des questions de cybersécurité.

Cet enjeu sociétal, je l'aborde avec trois casquettes : comme ancien maire de village d'abord ; comme législatrice, ensuite, en ma qualité de sénatrice et commissaire spéciale sur la sécurité numérique ; enfin en tant que première vice-présidente de la Commission Supérieure du Numérique et des Postes (CSNP). Car dans un État de droit, il faut un cadre juridique efficace, opposable, et proportionné : c'est pour cela que nous, parlementaires, travaillons à mieux protéger les composantes de la société contre la cybermenace au sens large.



Notre action se veut complémentaire d'un sursaut local que j'appelle de mes vœux. Car il convient de renforcer notre cadre normatif, sans occulter l'aspect financier qui pèse sur les collectivités, la cybersécurité ayant un coût.

Ce dont nous avons véritablement besoin, c'est d'une forme de révolution des pratiques et des mentalités que d'autres États ont déjà opérée chez eux, de l'Estonie à Israël. À nous acteurs publics de prendre clairement nos responsabilités, sans considérer la cybersécurité comme l'affaire des autres, et notamment des seules institutions sécuritaires. Développons les bonnes pratiques et restons agiles pour faire face aux pirates informatiques : face à leur imagination sans limite, affichons une détermination sans faille. Force doit rester à la loi, y compris dans le cyberespace. Renforçons la coopération entre public et privé, formons plus vigoureusement les fonctionnaires et gestionnaires de services informatiques des administrations et des collectivités. Ainsi nous serons à même de créer, tous ensemble, une culture de la défense numérique.

TOINE BOURRAT
Sénatrice des Yvelines

23% DES ATTAQUES CONCERNENT LES INSTITUTIONS TERRITORIALES, SOIT LES 2ÈME ORGANISATIONS LES PLUS CIBLÉES.

PLÉNIÈRE

COLLECTIVITÉS : COMMENT FAIRE FACE À LA CYBERMENACE ?

En ouverture des Assises Cybersécurité 2023, organisées par Seine-et-Yvelines Numérique, une table ronde est venue rappeler les enjeux et dresser un état des lieux de la menace pour les collectivités territoriales. Sans oublier d'ouvrir des pistes de réflexion et de donner des clés en matière de protection et de cyber-résilience.

La cybermenace se place aujourd'hui au cœur des préoccupations pour les collectivités, dont 13% sont chaque année touchées par une attaque[1]. Selon l'ANSSI[2], les acteurs territoriaux représentent les deuxièmes organisations les plus ciblées, concentrant 23 % des attaques. Le phénomène n'est pas nouveau mais il a pris, avec le télétravail et la situation géopolitique, des proportions réellement industrielles. Dans ce tableau, les communes de moins de 3 500 habitants, soit 91 % du tissu national, sont encore trop peu conscientes du danger : 65 % d'entre elles[3] considèrent en effet le risque cyber comme « nul voire faible ». Pour repousser l'échéance, ces collectivités invoquent quatre raisons : ce n'est pas leur métier, pas leur priorité, elles n'ont ni le temps, ni le budget. Pourtant, les cyberattaques n'arrivent pas qu'aux autres, comme le prouvent les nombreux exemples récents, à l'image de la ville de Chaville ou de l'hôpital Mignot à Versailles.

CYBERCRIMINALITÉ : UN ÉCOSYSTÈME TRÈS BIEN ORGANISÉ

Si les collectivités font partie des victimes les plus fréquentes, c'est notamment parce qu'elles se protègent encore trop peu. Un pirate informatique préférera cibler cent petites communes d'un coup (sachant que certaines paieront la rançon et qu'il pourra ainsi gagner autant d'argent, voire plus) qu'attaquer frontalement une grande ville mieux préparée. Il faut savoir que l'écosystème de la cybercriminalité est aujourd'hui très organisé. Il comprend de nombreuses sortes de hackers qui utilisent des modes opératoires variés, selon leurs objectifs. Pour pirater les collectivités, le phishing ou hameçonnage, via un email infecté, demeure la technique préférée des malfaiteurs. **En moins de dix minutes, une infrastructure peut ainsi se retrouver totalement chiffrée**, simplement parce qu'un collaborateur a ouvert une pièce jointe douteuse. Une fois le ver dans le fruit, les dégâts peuvent être absolument considérables, avec à la clé une désorganisation totale des services et la perte de données.

HOUILLES : DEUX ANS APRÈS, RETOUR D'EXPÉRIENCE

La commune yvelinoise de Houilles (35 000 habitants) a fait l'amère expérience d'une cyberattaque en 2021. Le maire de la ville, Julien Chambon, est revenu pour ces Assises sur cette expérience douloureuse mais formatrice alors qu'il était élu depuis quelques mois seulement. Il a d'abord souligné l'**extrême dépendance de toute l'activité municipale à la centaine de logiciels métier** utilisés par les équipes, et la prise de conscience qui a résulté de la crise traversée. Sans pour autant se voiler la face : deux ans après, un test de phishing a démontré que 40 % des agents cliquaient encore sur des liens potentiellement malveillants, d'où la nécessité de sensibiliser les équipes en continu. Julien Chambon a également évoqué la **difficulté à juger du bon niveau de ressources à allouer à la cyberprotection**, dans un contexte où l'exploitation même des systèmes est déjà très lourde financièrement pour les communes. Il a enfin expliqué à quel point il est **ardu de trouver un interlocuteur compétent et disponible** pour aider la municipalité à gérer techniquement la crise, dans l'urgence, afin de rétablir le service public.

PRÉPARER SA RÉSILIENCE AVEC UN PRA (Plan de Reprise d'Activité)

La question n'étant pas de savoir si une collectivité sera touchée, mais plutôt **quand**, chacune d'entre elle, quelle que soit sa taille, a intérêt aujourd'hui à **anticiper en effectuant des sauvegardes régulières** (back-up) et en **formalisant son plan de reprise d'activité**. En faisant certes appel à la technique, mais aussi au bon sens : quels sont les métiers qui doivent pouvoir redémarrer en premier ? Dans quel ordre ? Sur quoi se base-t-on pour tout reconstruire ? Cette dimension de **cyber-résilience** fait intrinsèquement partie de la cybersécurité et doit aujourd'hui prendre toute sa part dans les plans de sauvegarde des collectivités.

UNE NÉCESSAIRE MONTÉE EN PUISSANCE DE LA CYBERSÉCURITÉ

Les acteurs publics se trouvent au début d'une nouvelle ère où les **enjeux en matière de cybersécurité seront de plus en plus centraux**, d'autant que le nombre croissant d'objets connectés augmente chaque jour la surface d'attaque. Le territoire francilien va cependant pouvoir capitaliser sur les événements à venir, Coupe du monde de Rugby 2023 et Jeux Olympiques 2024, afin de monter plusieurs marches d'un coup pour être prêt à contrer la menace, toujours démultipliée à l'occasion de ce type de manifestation. Parallèlement, la réglementation tant française qu'européenne (Directive NIS2) va s'intensifier et les contraintes de sécurité se renforcer. Dans ce contexte, les collectivités doivent poursuivre leur chemin vers la **cyber-maturité** : un parcours sur lequel Seine-et-Yvelines Numérique peut les accompagner dans la durée.

1 & 3. source www.cybermalveillance.gouv.fr

2. Agence nationale de la sécurité des systèmes d'information

« Aujourd'hui, la cybersécurité est une priorité pour les collectivités. Le Conseil départemental des Yvelines est tout à fait conscient que de nombreuses communes n'ont ni la capacité financière, ni les ressources en ingénierie pour régler cette question. C'est pourquoi nous proposons, au travers de notre opérateur Seine-et-Yvelines Numérique, des solutions mutualisées et, de ce fait, accessibles au plus grand nombre. »

PIERRE BÉDIER
Président du Conseil départemental des Yvelines

JULIEN CHAMBON | Maire de Houilles (Yvelines)

« Au-delà de l'aspect technique, c'est dans la capacité à se relever et à faire preuve de résilience après une attaque, que réside à mon sens le véritable enjeu. Car l'humain reste au cœur de tous les processus. Il ne faut pas non plus croire qu'une crise subie prémunit nécessairement contre une future attaque : d'où l'importance de continuer à sensibiliser et à transmettre la mémoire de ce qui est advenu aux nouveaux arrivants. »

STÉPHANE BLANC | Président-fondateur d'AntemetA

« Les sauvegardes, ou back-up, constituent un enjeu clé en matière de cybersécurité. C'est la convergence de la sécurité et du secours qui fera l'efficacité de la restauration des systèmes d'information. La formalisation d'un plan de reprise d'activité constitue donc une nécessité en amont. »

DENIS BOYER

Officier de police judiciaire, expert en cybermalveillance et chargé de mission au sein du dispositif Cybermalveillance.gouv.fr

« L'un des soucis principaux pour les collectivités réside dans des pratiques potentiellement dangereuses comme le partage de mots de passe ou d'ordinateurs, mais aussi dans une frontière parfois trop floue entre sphère privée et professionnelle. Autant de paramètres qui augmentent la surface d'attaque pour les pirates. »

ATELIER 1

CYBERSÉCURITÉ : DE QUELS MÉTIERS AI-JE BESOIN DANS MA COLLECTIVITÉ ?

Animé par
Ludovic Dubosc
RSSI Seine-et-Yvelines Numérique

QUATRE FAMILLES DE MÉTIERS CYBERSÉCURITÉ AU SERVICE DES COLLECTIVITÉS

1 **Gestion de la sécurité et pilotage des projets**

Il s'agit du directeur cybersécurité ou du RSSI (Responsable de la Sécurité des Systèmes d'Information). Dans une petite structure, cela peut être un CSSI (Chargé de la Sécurité des SI), soit un agent ayant une appétence pour le sujet et qui sera un porteur logique de la démarche, voire un alertant.

2 **Conception et maintien d'un SI sécurisé**

On parle ici de l'auditeur de sécurité organisationnelle et technique, qui va opérer un diagnostic des SI pour améliorer la résilience. Dans une plus grande collectivité, c'est un administrateur de solutions de sécurité. Enfin, pour les plans à grande échelle, on fait appel à un chef de sécurité projet, et éventuellement à un architecte sécurité.

3 **Gestion des incidents et des crises de sécurité**

Fonction assurée par un gestionnaire spécialisé et par des analystes.

4 **Conseil, services et recherche**

Prestations délivrées par des consultants en cybersécurité et des formateurs.

SIX PILIERS POUR LA MAÎTRISE DES RISQUES CYBER (ISO 27001)

1 **Maîtriser ses risques**

Connaître son niveau de risque et identifier ses ressources critiques, afin de prioriser les phases de la démarche cybersécurité.

2 **Maîtriser les accès**

Aujourd'hui, les SI sont ouverts, il est donc important de déterminer qui a accès à quoi, et quels sont les niveaux d'accès pertinents selon les collaborateurs.

3 **Maintenir le SI en conditions de sécurité et de détection**

4 **Maîtriser le corpus documentaire**

Analyse de risque, cartographie de sécurité, procédures opérationnelles.

5 **Maîtriser les compétences et sensibiliser les équipes**

6 **Choisir la voie de l'amélioration continue**

La cybersécurité est itérative : elle se construit patiemment, avec l'ensemble des équipes.

ZOOM SUR

LE RSSI, GARANT DE LA CYBERSÉCURITÉ DE LA COLLECTIVITÉ

Véritable chef d'orchestre, le Responsable de la Sécurité des Systèmes d'Information assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il préconise les actions à mener afin de préserver la continuité des SI, vérifie que la politique de sécurité des SI est bien appliquée, et si besoin, accompagne la collectivité dans sa définition. Enfin, il met en place et anime les comités dédiés à la cybersécurité, définit et maintient le corpus documentaire dédié.

LE DPO, AU SERVICE DE L'INTÉGRITÉ DE VOS DONNÉES

Le Délégué à la Protection des Données (ou DPO) veille au respect de la réglementation et se veut le point d'entrée institutionnel de la collectivité vis-à-vis de la CNIL (Commission nationale de l'informatique et des libertés). Il met en place ou maintient des registres de traitement (droits individuels, violation des données, transferts de données hors Union européenne, etc). Il est également l'interlocuteur clé concernant la durée d'archivage et de conservation des données. Enfin, il sensibilise les équipes aux exigences du RGPD (Règlement général de protection des données).

BON À SAVOIR

C'EST L'ENSEMBLE DE SON ÉCOSYSTÈME QU'IL FAUT SÉCURISER

Pour entrer dans vos systèmes d'information, les hackers ciblent votre écosystème au global, donc ne vous contentez pas de sécuriser votre périmètre : ayez un regard à 360° sur l'ensemble des tiers avec lesquels vous interagissez.

SOYEZ TOUJOURS ALERTÉ PAR LA CONNOTATION D'URGENCE D'UN MESSAGE INHABITUEL

Le milieu de la cybercriminalité se professionnalise et les campagnes d'hameçonnage sont de plus en plus crédibles. Leur point commun : elles jouent en général sur la notion d'urgence, ce qui fait perdre leur bon sens aux personnes ciblées.

ATELIER 2

CYBERSÉCURITÉ : COMMENT ET POURQUOI SENSIBILISER MES AGENTS ?

Animé par

Renaud Fourtalin,
consultant cybersécurité
Phosforéa
et Thomas Robert,
Business Development and
Operations Director Phosforéa

DÉCRYPTER LA MENACE

La démarche de sensibilisation commence en général par une **prise de conscience des risques**. À ce titre, il est bon d'expliquer aux agents que leur collectivité peut être touchée d'un instant à l'autre, avec à la clé une désorganisation totale de l'activité et des conséquences parfois graves, des serveurs paralysés et des données piratées. Ces actions sont le fait d'acteurs assez divers, du hacker récréatif aux réseaux mafieux, et ont des objectifs variés, de l'appât du gain à la déstabilisation politique. Les formats de cyberattaques, quant à eux, vont du classique phishing au vol de mot de passe, en passant par le chantage (ransomware).
Si les collectivités territoriales sont particulièrement touchées, c'est notamment parce que la majorité d'entre elles **autorisent un accès à leurs systèmes d'information depuis un PC (83 %), un smartphone ou tablette (75 %)**. Or elles sont seulement 35 % à chiffrer leurs données, ce qui élargit la zone d'attaque et explique l'engouement des cyberpirates pour ce type de cibles.

SIX CONSEILS POUR UNE CAMPAGNE DE SENSIBILISATION RÉUSSIE

1. S'inscrire dans la durée

On est davantage sur une course de fond que sur un sprint ! Il est nécessaire de mettre en place une démarche de longue haleine, pour faire évoluer les comportements et les compétences des agents, mais aussi pour identifier les risques associés à chacun d'entre eux en fonction de leur métier.

2. Susciter et maintenir l'attention des apprenants

C'est-à-dire s'adapter en termes de pédagogie aux différentes personnes à sensibiliser, en utilisant des supports variés (capsules, vidéos, e-learning…) et en menant des actions qui engagent les participants (quiz, jeux).

3. Mixer actions en présentiel et e-learning

En présentiel, il est possible de toucher des gens qui n'ont pas ou très peu accès à un PC : cela peut être via une campagne d'affichage ou bien en organisant des jeux, comme celui que Phosforéa a développé en s'inspirant du *1000 bornes*.

4. Bien choisir ses supports de communication

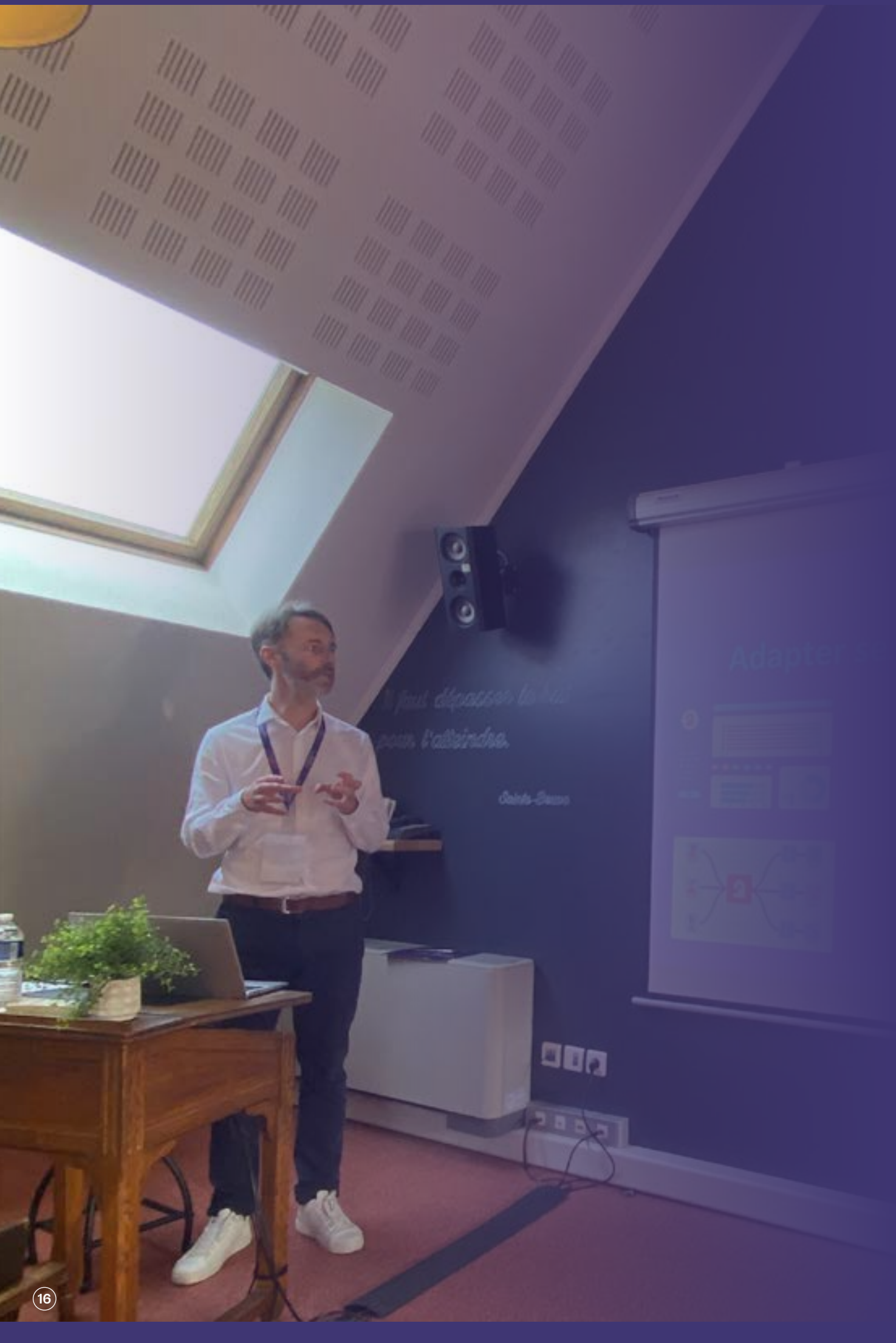
Affichage dans les ascenseurs, emailings, fond d'écran événementiel, prise de parole d'un sponsor en interne : il existe de nombreux moyens de capter l'attention des agents.

5. Mesurer les progrès et la performance

En définissant des critères et en analysant la participation des agents (leur niveau d'assiduité et les contenus visionnés, les réactions, l'application ou non des apprentissages et, bien entendu, l'impact sur la diminution de la menace cyber pour l'organisation).

6. Adapter les actions au niveau de connaissance des cibles

Cela implique d'identifier les besoins afin de choisir des contenus pédagogiques adaptés.



ZOOM SUR

L'OFFRE DE SENSIBILISATION PHOSFORÉA CO-CONSTRUITE AVEC SEINE-ET-YVELINES NUMÉRIQUE

Spécialement pensée et négociée par le syndicat à destination de ses adhérents, cette offre comprend :

L'accès à une plateforme de e-learning pendant 12 mois en mode SaaS[1] pour un nombre défini d'apprenants.

10 contenus de sensibilisation finement sélectionnés et étudiés par les équipes pédagogiques de Phosforéa en fonction de la cyber-maturité moyenne observée dans les collectivités.

Le **support technique** et **l'accompagnement** par un chef de projet attitré tout au long du projet.

Un suivi individuel des apprenants au moyen de tableaux de bord, et la possibilité de relancer individuellement les apprenants selon leur avancement dans la démarche.

L'édition d'une attestation de suivi par collaborateur à l'issue du parcours.

1. Le mode SaaS permet aux entreprises de s'abonner à un logiciel à distance plutôt que de l'acquérir et l'installer en interne.

ATELIER 3

RÉSILIENCE CYBER : QUELLES SONT LES MESURES ESSENTIELLES QUE JE DOIS PRENDRE POUR ME PRÉPARER ?

Animé par

Patrice Duhem
consultant cybersécurité du cabinet de conseil et audit cybersécurité on-x

LES QUATRE PRÉALABLES À TOUTE DÉMARCHE CYBERSÉCURITÉ

Comme tout chantier d'envergure, une démarche cybersécurité se prépare.

1. **Avoir conscience du risque et de l'importance du sujet** : en effet, une collectivité, même petite, est une cible potentielle car elle détient des données qui ont une valeur marchande.

2. **Faire en sorte que la démarche soit soutenue au plus haut niveau**, par le maire ou le président, afin de démontrer la volonté forte de l'organisation. À ce titre, la majorité des PSSI (politiques de sécurité des systèmes d'information) s'ouvrent d'ailleurs sur une page où le dirigeant exprime son engagement.

3. **Dégager un budget dédié**, afin de se donner les moyens de se protéger.

4. **Structurer sa démarche en fonction des spécificités de son système d'information (SI),** des objectifs de service public de la collectivité et des données sensibles qu'elle manipule, mais aussi définir clairement les rôles et responsabilités de chacun.

COMMENT ÉVALUER LA MATURITÉ CYBERSÉCURITÉ DE SON ORGANISATION ?

La première étape de la démarche consiste en un **état des lieux**, qui prend la forme d'un **audit de maturité cyber**. De quoi est constitué mon SI ? Quel est son périmètre exact ? Avec qui interagit-il ? Comment est-il protégé ? L'ANSSI (Agence nationale de la sécurité des systèmes d'information) propose deux guides afin d'encadrer cette phase : pour les petites collectivités, un guide des TPE recensant les 13 règles d'hygiène numérique essentielles et, pour les collectivités plus importantes, un guide comprenant 42 règles. La norme ISO 27001 liste, quant à elle, 114 règles qui sont cependant plus adaptées aux collectivités les plus importantes en taille.

L'audit va, dans un premier temps, **évaluer les forces et faiblesses** sur le périmètre défini, et **mettre en lumière les vulnérabilités** de l'organisation, soit les points d'entrée possibles pour les cyberattaquants. De ce constat découlera enfin un **plan d'action**.


Guide d'hygiène de l'A
(42 règles)
aluer ses
orces et
iblesses

ZOOM SUR

LES RÉPONSES AUX VULNÉRABILITÉS IDENTIFIÉES PAR L'AUDIT CYBER

DIMENSION TECHNIQUE

Il s'agit des **outils et applications** : antivirus, firewalls, segmentation des réseaux pour éviter la propagation des attaques, sécurisation des postes de travail, gestion des accès, etc.

DIMENSION HUMAINE

Près de 80 % des cyberattaques résultent d'une négligence humaine : la sensibilisation reste donc un maillon essentiel de la démarche. Pour être efficace, celle-ci doit être menée en continu, régulièrement, pour ancrer les bons réflexes et embarquer les nouveaux arrivants dans l'organisation. Le fait d'informer et de préparer les esprits permettra aussi de minimiser le choc psychologique si une attaque se produit, ce que les collaborateurs peuvent très mal vivre si rien n'a été anticipé.

DIMENSION ORGANISATIONNELLE

Pour la mettre en œuvre, le RSSI (responsable de la sécurité des SI) va s'appuyer sur un SMSI (système de management du SI) et sur une PSSI (politique de sécurité des systèmes d'information). Cette dimension comporte une importante composante communication, avec par exemple la mise en place de correspondants sécurité dans les directions métier. Elle se traduit aussi par des chartes et des procédures. Enfin, elle prépare à la gestion de crise en définissant le PCI (plan de continuité informatique) et le PRI (plan de reprise informatique) qui seront d'un grand secours en cas d'attaque.

SUR LA DURÉE : S'ENTRAÎNER ET SE FAIRE ACCOMPAGNER

La consolidation des acquis en matière de cybersécurité passe par un **entraînement de l'organisation et des équipes**, comme pour des sportifs, avec notamment des tests de phishing (ou hameçonnage), des **simulations pour éprouver la procédure** de crise prévue au PCA, enfin des **tests de restauration** pour être sûr que la collectivité sera capable, le moment venu, d'utiliser ses sauvegardes. Autant d'actions pour lesquelles **Seine-et-Yvelines Numérique propose à ses adhérents un accompagnement**, avec des prestations sélectionnées et négociées auprès de partenaires qui connaissent le monde des collectivités et ses spécificités.

ATELIER 4

COMMENT ET POURQUOI INTÉGRER LA CRISE CYBER DANS MON PLAN COMMUNAL DE SAUVEGARDE ?

Animé par

Thierry Cornu

directeur conseil et audit du cabinet on-x

LE PCS, UN OUTIL FONDAMENTAL

Les Plans Communaux de Sauvegarde (PCS), créés par le législateur en 2004, avaient originellement pour but de **préparer les communes** à réagir à des événements extraordinaires. Ils étaient initialement axés sur les problématiques de protection civile, notamment dans l'éventualité d'une catastrophe climatique de type inondation. Si la menace cyber ne présente que rarement un risque direct pour la population, il est cependant pertinent d'intégrer aujourd'hui cette dimension dans les PCS. En effet, **l'organisation de crise déjà définie dans les PCS constitue une excellente base** sur laquelle greffer des mesures spécifiques à la cybersécurité.

PREMIERS RÉFLEXES EN CAS D'ALERTE CYBER

Pour mettre en place les premiers secours en cas d'alerte, la collectivité doit disposer d'un **collaborateur formé aux gestes d'urgence**, souvent le responsable informatique, et de consignes précises pour les personnes chargées de la communication avec le public.
Autre enjeu : **avoir prévu des sauvegardes de toutes les composantes du système d'information** (SI), mais aussi **savoir dans quel ordre les restaurer**. La collectivité doit également pouvoir **remonter les traces**, soit les journaux techniques de tout ce qui s'est passé sur ses serveurs, afin d'analyser comment la crise est arrivée et quels sont ses impacts. Enfin, il est impératif de **prévoir à l'avance des moyens de communication alternatifs** pour permettre aux collaborateurs de continuer à travailler ensemble même en cas de paralysie totale du SI, avec notamment un mémo recensant les contacts d'urgence et les procédures à suivre (sous format papier).

SANS CESSE REQUESTIONNER L'EXISTANT

En amont, cela signifie **vérifier régulièrement que la cartographie des SI est à jour**, **ajuster ses PCI et ses PRI** (plans de continuité et de reprise informatique), **identifier les intervenants externes** qui pourront apporter de l'aide le moment venu, enfin avoir **préparé les outils de communication et de gestion de crise**, en lien avec ce qui existe déjà dans le PCS. Pour mettre à l'épreuve l'organisation de gestion de crise, la **conduite d'exercices réguliers** est recommandée. Cela peut aller de la simulation sous forme d'un jeu (type *serious game*) avec un comité restreint de collaborateurs dits « primo-intervenants », jusqu'à un test de plus grande ampleur avec restauration de sauvegardes, ou encore une vérification des procédures d'intervention de l'infogérant.

LE PCS, UN SOCLE TRÈS UTILE POUR GÉRER LA CRISE CYBER

Dans les communes ayant déjà défini leur PCS, l'**organisation de la gestion de crise est déjà formalisée et constituera un socle** sur lequel s'intègrera naturellement un volet cybersécurité. La cellule de crise stratégique décisionnelle du PCS se verra alors complétée par une **cellule de crise cyber et IT**. Cette dernière, composée des spécialistes métier, pilotera les investigations, la remédiation et les opérations de reconstruction du SI.

Seine et Yvelines
Numérique

L'innovation au service de tous

Seine-et-Yvelines Numérique
15 bis, avenue du Centre
78 280 Guyancourt

www.sy-numerique.fr
contact-syn@sy-numerique.fr