LA CYBERSÉCURITÉ DANS LES ADMINISTRATIONS

29 janvier 2026

Par Christophe GAIE

Conférence réalisée dans le cadre du séminaire
« Cybersécurité : une guerre toujours gagnable ? »

Sommaire

1. Qui suis-je ?
2. Quelles spécificités de la sphère publique ?
3. Quels sont les risques cyber ?
4. Comment se protéger
5. Comment gérer une crise cyber ?
6. Conclusion

Qui suis-je ?

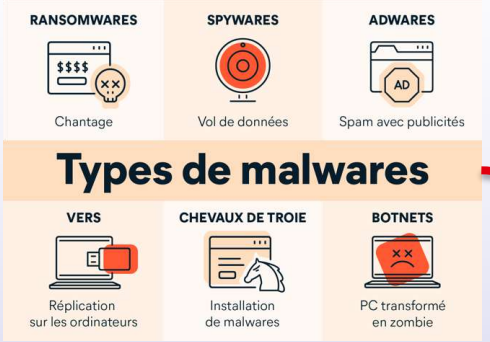
- **Emploi actuel** : Chef de division au SGDSN / OSIIC (depuis 2023)
  - Plus de cent projets informatiques
  - Management de 5 bureaux et 70 personnes
- **Précédents postes :**
  - Chef de bureau Ministère de la Transformation Publique (2 ans et demi)
  - Chef de projet Premier Ministre (1 an)
  - Chef de projet Ministère des Finances (4 ans et demi)
  - Architecte informatique Ministère des Finances (5 années)
- **Parcours académique :**
  - Diplômé de l'Ecole de Guerre-Terre, Auditeur IHEDN certifié
  - Spécialisation pour le Ministère des Finances
  - Doctorat en Télécommunications
  - Ingénieur en Télécommunications
- **Loisirs :**
  - Sports (triathlon, course à pied, natation, cyclisme)
  - Ancien arbitre national (18 ans)
  - Recherche sur la thématique du gouvernement électronique et de la défense nationale

Christophe GAIE

https://www.linkedin.com/in/christophegaie/

https ://scholar.google.com/citations?user=_vBNVlkAAAAJ

QUELLES SPÉCIFICITÉS DE LA SPHÈRE PUBLIQUE ?



Pourquoi la Cybersécurité est-elle critique pour le Secteur Public ?

- **Sensibilité des données traitées par l'État**
  - Informations personnelles (revenus, santé, …)
  - Informations stratégiques (militaires, nucléaires, sécurité nationale, …).

- **Impact majeur sur la société:**
  - Interruption de services critiques (ministères, collectivités, hôpitaux …)
  - Divulgation de données sensibles (maladie, patrimoine, …) avec impact personnel
  - Perte de confiance des citoyens, atteinte à l'image des administrations

- **Augmentation des cyberattaques (exemple des rançongiciels)**

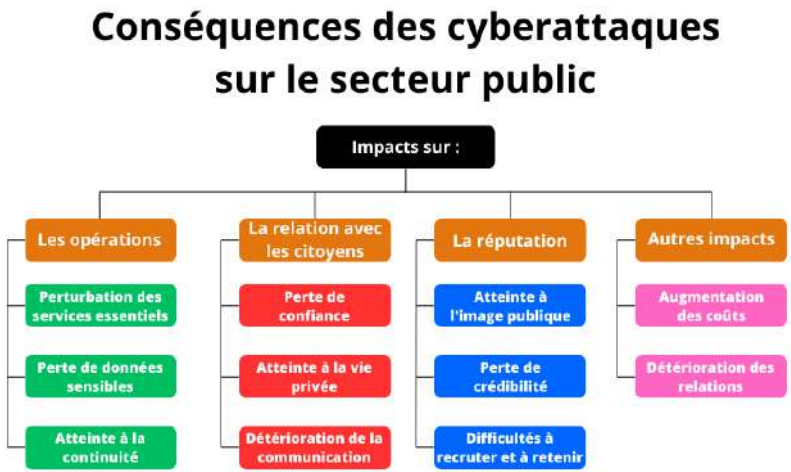
Secteur	Attaques Confirmées	Dossiers Affectés	Demande de Rançon Moyenne
Agences Gouvernementales	179	1,5 millions	2,3 millions de dollars
Santé	181	25,6 millions	5,7 millions de dollars
Éducation	116	1,8 millions	847 000 dollars

https://www.comparitech.com/news/ransomware-roundup-2024-end-of-year-report/

Point clé : les entités publiques sont des **cibles privilégiées** en raison de la **richesse des données** qu'elles détiennent et de **l'impact potentiel sur la société**.

Pourquoi la Cybersécurité est-elle critique pour le Secteur Public ?

- **Des conséquences multiples avec un impact particulier sur le fonctionnement des services …**



Source : https://blog.httpcs.com/secteur-public-cybersecurite/

- **… et des impacts financiers majeurs !**

Exemple de l'hôpital Mignot dans les Yvelines :

« La cyberattaque a occasionné de nombreux coûts que l'hôpital a du mal a supporter seul :

- *une perte de 7 millions d'euros de recettes due à la diminution du nombre de personnes hospitalisées en 2023,*
- *à laquelle s'ajoutent 3 millions dépensés cette même année auprès de prestataires informatiques*
- *et encore 3 millions d'investissement dans ce domaine. »*

Source : https://www.francebleu.fr/infos/sante-sciences/deux-ans-apres-avoir-ete-victime-d-une-cyberattaque-l-hopital-mignot-dans-les-yvelines-toujours-en-difficulte-4685429

Quelques attaques contre les entités publiques

Tout peut être attaqué !

07/11/2024

Trente hôpitaux français victimes d'une cyberattaque en deux ans

23/11/2022

Le site web du Parlement Européen touché par une cyberattaque

11/01/2022

Une cyberattaque met hors ligne tout un district scolaire aux États-Unis

10/09/2024

548 événements de cybersécurité en lien avec les Jeux Olympiques

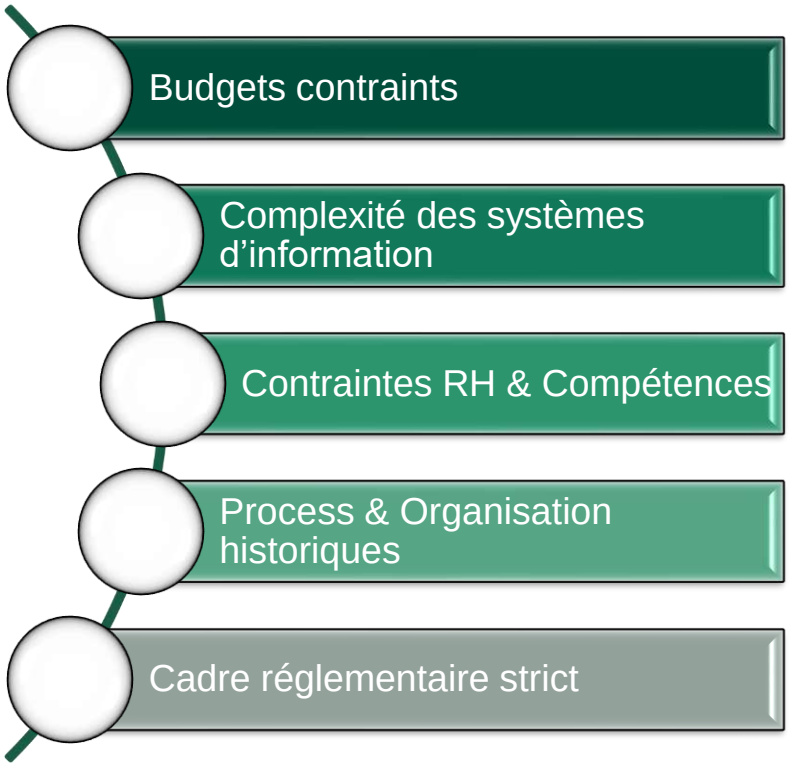
14/03/2024

La cyberattaque contre France Travail concerne 43 millions de personnes

20/05/2025

Le département des Hauts-de-Seine paralysé par une cyberattaque

Les Défis Spécifiques au Secteur Public



- Budget SI de 650 Millions € pour la Douane et la DGFiP sur 9,5 Mds € (soit 7%)
- à comparer à BNP Paribas qui a stabilisé ses dépenses IT (aux environs de 16%) de son PNB, soit env. 7,5 Md€

- La Cour des comptes a souligné le poids des dépenses d'exploitation et de maintenance de la DGFiP 62 %, les logiciels sont souvent spécifiques
- Selon un rapport de 2023 du CIGREF (Club Informatique des Grandes Entreprises Françaises), le ratio RUN/BUILD est de 64/36.

- Règles de recrutement et de formation de la fonction publique
- Contraintes liées à la commande publique

- Arrêté du 5 janvier 1990 modifiant l'arrêté relatif au traitement informatisé d'impôt sur le revenu à la direction générale des impôts (fichier POTE, tech COBOL)
- Décret n°82-103 du 22 janvier 1982 relatif au répertoire national d'identification des personnes physiques.

- Conformité aux normes (RGS, RGAA, RGI, RGESN, RGPD, NIS 2, etc.) qui peut être complexe et consomme beaucoup de ressources.

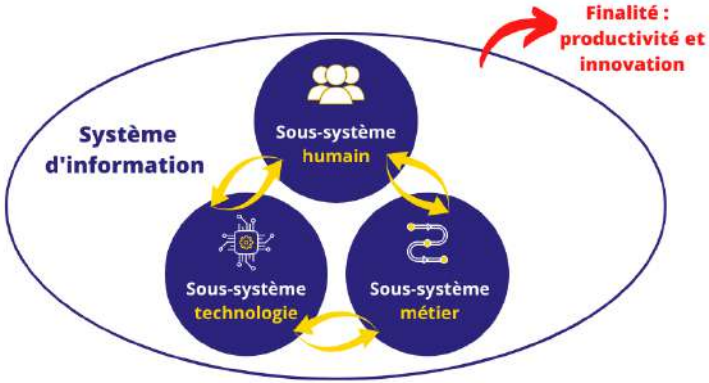
QUELS SONT LES RISQUES CYBER ?

Source : freepik

Quels sont les enjeux de sécurité informatique ?

Un système d'information (SI) s'appuie sur **plusieurs composantes**

- Chacune de ces composantes du SI possède ses propres forces et faiblesses, ainsi que ses propres caractéristiques et usages.
- Chaque composant du système d'information a également ses propres exigences en matière de sécurité.



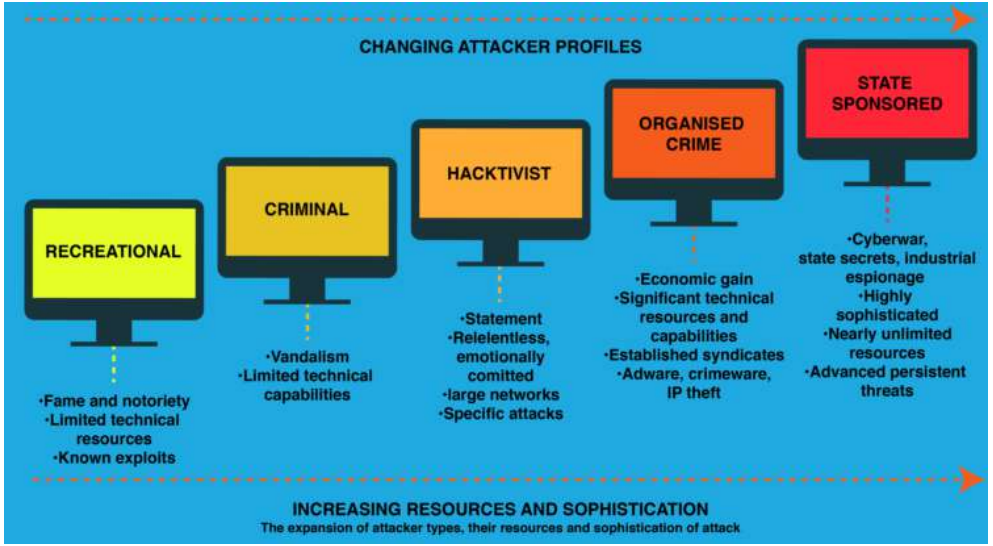
1) Le sous-système humain
Ce sont toutes les **personnes** nécessaires pour faire fonctionner et gérer le système, ainsi que toute personne qui interagit avec le SI.

2) Le sous-système technologie
Le **matériel informatique** est l'équipement physique utilisé pour la collecte, le stockage, le traitement et la diffusion de l'information.
Les **logiciels** sont les programmes qui s'exécutent sur le matériel information..
Les **réseaux** sont les moyens de télécommunications utilisés pour transmettre une donnée (réseau local, internet, etc.).

3) Le sous-système métier
Les processus métier sont l'ensemble des **tâches et flux** de travaux impliquées directement et indirectement dans la chaine de valeur de l'entreprise.

Qui peut attaquer votre système ? Pourquoi ?

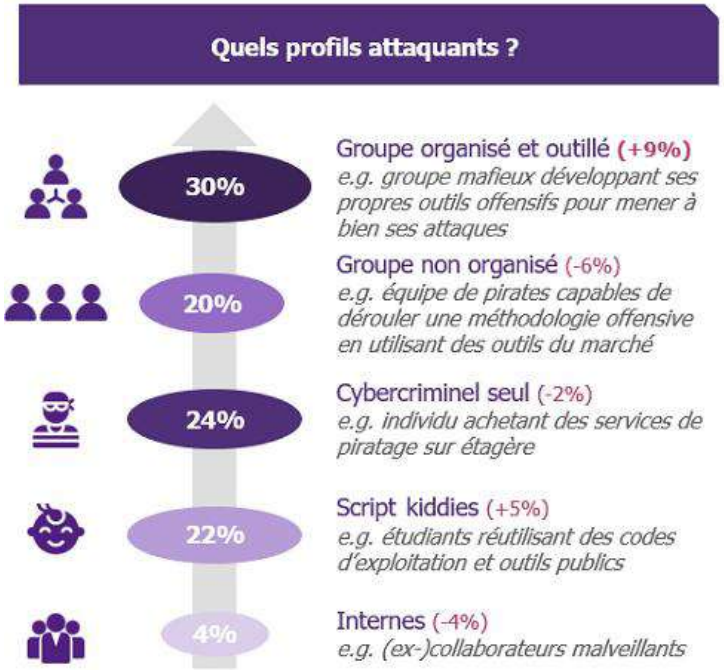
- Il existe **de multiples motivations** et profils d'attaquants
- Il est important d'**identifier le potentiel des risques** ainsi que les vulnérabilités
- L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) recommande d' **utiliser EBIOS Risk Manager** (EBIOS RM)
  - mettre en place ou renforcer un processus de gestion du risque numérique au sein d'une organisation ;
  - évaluer et traiter les risques liés à un projet numérique, notamment en vue d'une accréditation de sécurité ;
  - définir le niveau de sécurité à atteindre pour un produit ou un service en fonction de ses cas d'usage et des risques.
- La méthode est conforme à la **norme ISO 27005**
- https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/



https://www.futurelearn.com/info/courses/the-cyber-security-landscape-sc/0/steps/60317

Qui peut attaquer votre système ? Pourquoi ?

- Des profils d'attaquants qui évoluent au cours du temps
- Accroissement des moyens des attaquants, et structuration de leur organisation
- Facilitation par l'arrivée des outils d'intelligence artificielle et les réseaux sociaux



https://www.globalsecuritymag.fr/Cyberattaques-en-France-3-mois,20201014,103808

COMMENT SE PROTÉGER ?

Image générée par Gemini 2.5 Pro

Comment se protéger des erreurs humaines ?

Constat : L'erreur humaine est responsable de 90 % des cyberattaques (…) que ce soit par le biais de l'hameçonnage (phishing), de la mauvaise gestion des mots de passe ou encore d'une mauvaise protection.[1]

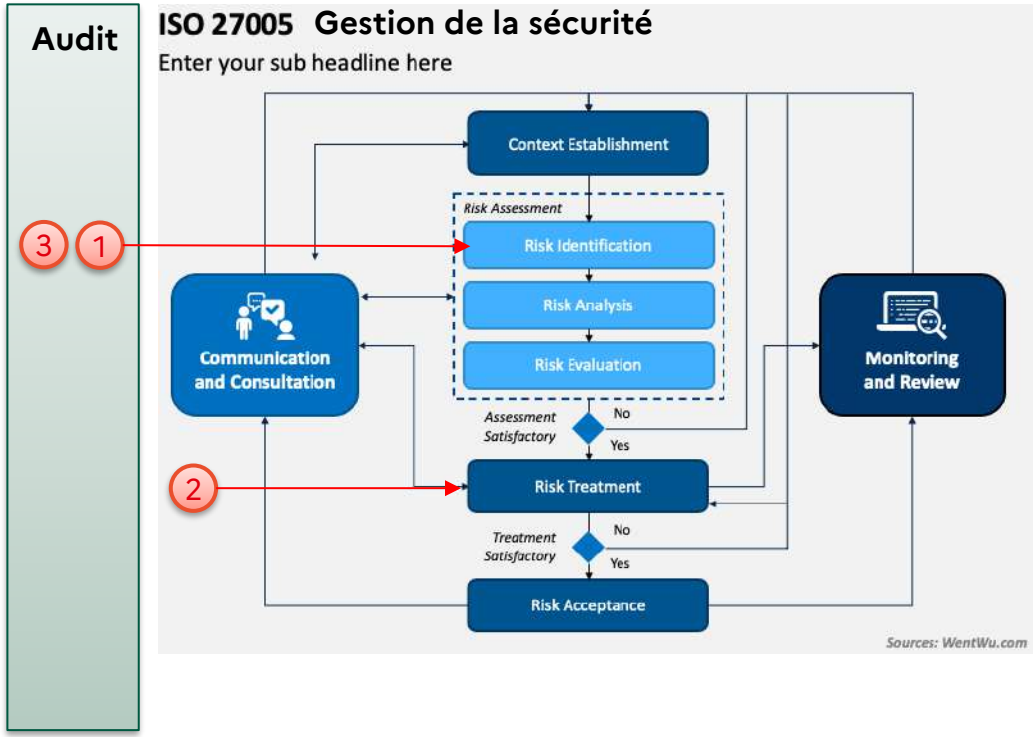
Actions à envisager (liste non exhaustive) :

- Campagnes de sensibilisation régulières et interactives.
  - SensCyber: Apprendre et tester vos connaissances - Assistance aux victimes de cybermalveillance
- Formations adaptées aux rôles (utilisateurs finaux, IT, managers).
  - Le MOOC SecNumacadémie | ANSSI
- Simulations d'attaques (phishing test).
  - Définir les acteurs, le processus, les outils et être pédagogique (s'inspirer de la démarche incendie)
- Culture de la vigilance et du signalement.
  - Désigner des points de contact, des adresses mails de contact et assurer un feedback

[1] Source : https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/reduire-le-risque-derreur-humaine

Comment protéger les applications informatiques ?

- **Avant de déployer** une application informatique, il est obligatoire de s'identifier des risques et protéger contre ces la plupart nocif ceux
- Le processus peut nécessiter de réaliser un audit de sécurité pour identifier des vulnérabilités
- Exemple :
  - J'ai géré une nouvelle application intitulée SICARDI qui permet de suivre les compétences des fonctionnaires du Ministère des Finances français
  - Un audit de sécurité a été réalisé en octobre 2022 et a décrit quelques vulnérabilités (1)
  - Les vulnérabilités ont été prises dans prise en compte dans le processus de réduction des risques
  - Les développeurs ont corrigé le code entre octobre 2022 et janvier 2023 (2)
  - Un nouvel audit a été réalisé et a confirmé la conformité en janvier
  - L'application a donc été mise en production en février 2023 (3)



Comment mettre en œuvre la sécurité dans les projets informatiques ?

La cyber-sécurité outils et appareils (exemple)

SonarQube pour analyser le code source

OWASP ZAP pour détecter potentielles vulnérabilités des applications Web

Cyberwatch pour détecter des potentielles vulnérabilités des systèmes informatiques (Linux, …)

HarfangLab logiciel de Cybersécurité conçu pour détecter et neutraliser les attaques informatiques visant les serveurs et les postes de travail.

S3Box et Tyrex offrent deux solutions de stations blanches pour vérifier si des clés USB sont contaminées. Le mieux restant de ne pas en utiliser ☺

Anticiper et se préparer à affronter une crise cyber

Recommandations de l'ANSSI

La gestion d'une crise cyber ne s'improvise pas : il est nécessaire de se préparer, s'outiller, s'entrainer et de connaître les bonnes pratiques de gestion de crise. Pour ce faire, il convient de :

- S'assurer de l'existence d'un **plan de continuité d'activité (PCA)** robuste aux cyberattaques et d'un **plan de reprise d'activité (PRA)** ;
- Préparer les capacités de **réponse à incident**, y compris en cas de perte des moyens informatiques et de communication nominaux ;
- Anticiper les menaces cyber et adapter le dispositif de crise à ces **menaces** ;
- Formaliser une **stratégie de communication** cyber ;
- **S'entrainer** pour pratiquer et s'améliorer ;
- Contractualiser le cas échéant des **prestations de réponse à incident** et souscrire une assurance cyber.
- Pour que ce dispositif soit robuste, il doit s'appuyer sur des **mesures de gouvernance, de protection et de défense** qu'il vient compléter.

Pour anticiper une crise majeure ayant un impact possible sur la continuité économique et sociale du pays, l'Etat a élaboré dans le cadre de sa politique de défense nationale les plans VIGIPIRATE et PIRANET : Plans gouvernementaux

https://cyber.gouv.fr/anticiper-et-gerer-une-crise-cyber

COMMENT GÉRER UNE CRISE CYBER ?

Image générée par Gemini 2.5 Pro

Gérer une crise cyber

Recommandations de l'ANSSI

Lorsqu'un évènement déstabilisateur survient, il est toujours difficile de piloter efficacement son dispositif de crise. **Le bon sens, la réactivité, l'adaptabilité et l'endurance des équipes** de gestion de crise face à une situation inédite en facilitent la gestion.

Les aspects suivants sont des incontournables pour réduire les impacts négatifs de la crise cyber sur l'organisation :

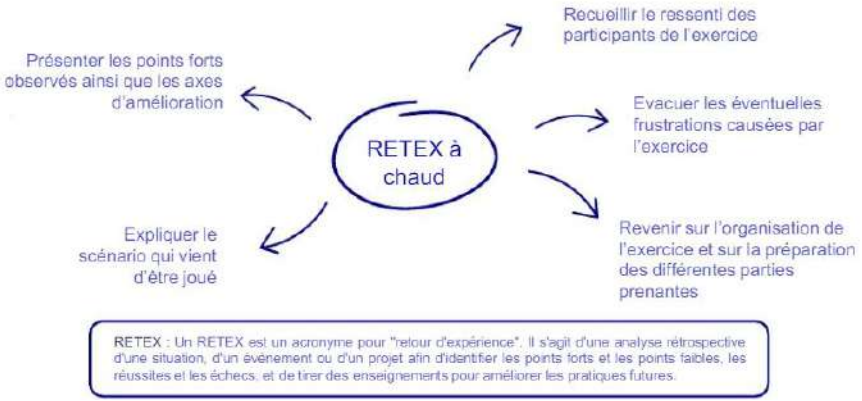
- Bien gérer les **seuils d'escalade** jusqu'au passage en crise ;
  - ✓ *Faire la distinction entre un ralentissement (surcharge) et un dysfonctionnement (plus d'accès aux serveurs)*
- Articuler le **pilotage** de la crise (métiers) et la **réponse** à incident (technique) ;
  - ✓ *Ceux qui pilotent ne sont pas ceux qui font ! Cela garantit des garde-fous et permet d'éviter les surincidents*
- **Coordonner et soutenir l'action** des équipes du dispositif de réponse ;
  - ✓ *Faire un plan et s'y tenir. Mettre en place des points de contrôle. Assurer la relève des astreintes, plateaux repas, le repos, …*
- Communiquer efficacement pour **maintenir la confiance** avec les acteurs internes et externes;
  - *Ne jamais mentir (ligne rouge !!!). Par contre on est parfois amené à distiller l'information pour gagner du temps opérationnel*
- **Impliquer les métiers** dans la construction du plan de remédiation et de relance d'activité ;
  - *Certaines tâches ne sont pas uniquement informatique. Des contournement organisationnels sont parfois possible (excel, word…)*
- **Tirer les leçons** à chaque activation de la cellule de crise.
  - *Réaliser un RETEX, ne pas commettre la même erreur*

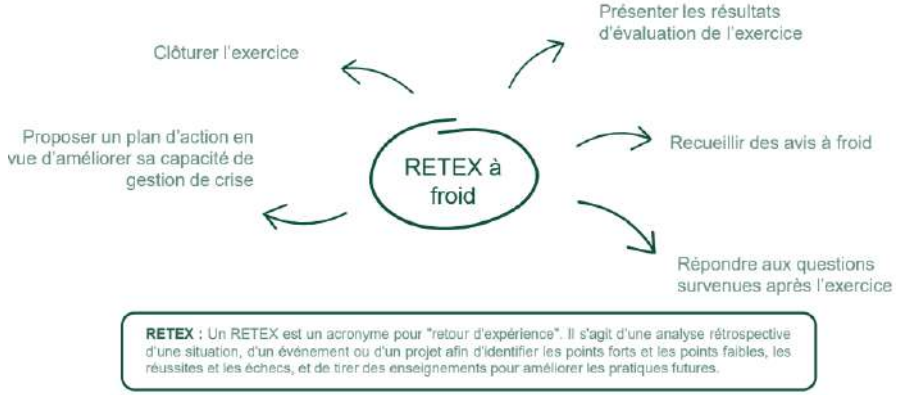
Il faut savoir que chaque crise fait l'objet d'un retour sur expérience qui demande par la suite une nouvelle analyse de sa gouvernance afin de structurer de nouveau ses mesures de sécurités. En effet, suite à une crise, il est nécessaire de mettre en place des actions immédiates.

Une crise bien gérée est également l'opportunité pour durcir durablement ses systèmes d'information et renforcer son organisation face aux cyberattaques.

anssi-guide-organiser-un-exercice-de-gestion-de-crise-cyber-v1.0.pdf

Gérer une crise cyber – Focus RETEX





A chaud, donc dans l'action ou juste après, le retour d'expérience **porte sur l'immédiat.**

Il aboutit soit à des **mesures probablement temporaires**, soit à des ébauches de solutions qu'il conviendra de confirmer.

A froid, les acteurs du retour d'expérience bénéficient **de plus de temps**. Ils s'appuient sur **davantage de données.**

Et, surtout, il est possible de considérer un problème dans son ensemble pour aboutir à des **propositions plus globales**.

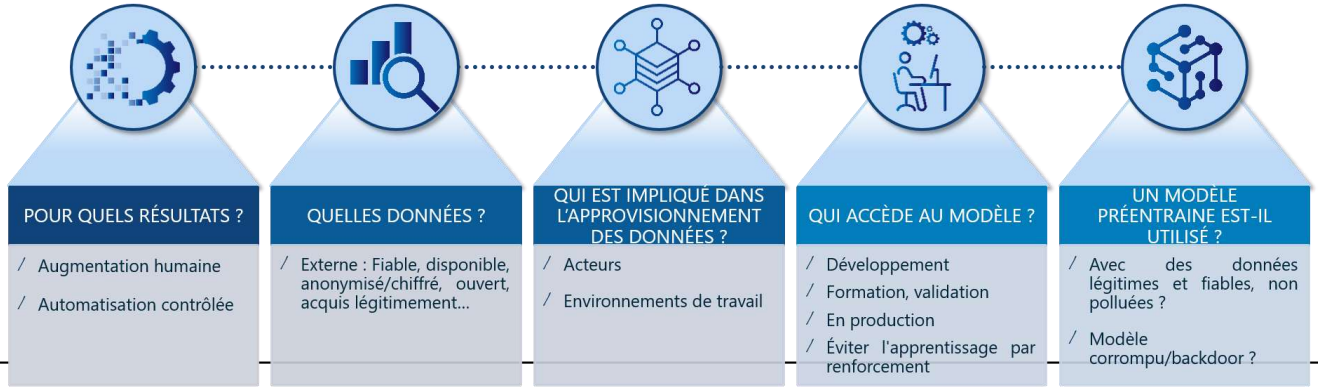
Ne pas commettre les mêmes erreurs
S'améliorer pour mieux gérer la prochaine crise

La sécurité et l'IA

- Injection de données
- « Vol » d'information (les agents dévoilent des secrets …)
- Perte de maîtrise des systèmes

- Optimisation des processus métiers
- Détection d'intrusion
- Identification des vulnérabilités
- Auto-adaptation des systèmes

Bonnes pratiques



Source: pixabay.com

Conclusions

- La sécurité est un **INVESTISSEMENT** pour assurer la sécurité de l'organisation, protéger ses donner et ses services
- La sécurité est une **PRÉOCCUPATION MAJEURE** des équipes projets et des DSI qui y consacrent une importante énergie
- La sécurité doit être prise dans compte **DÈS LE DÉBUT et TOUT AU LONG** du projet. Elle s'appuie par ailleurs sur les directions métiers qui assument les risques.
- La sécurité nécessite d' **AJUSTER** l'organisation des équipes projets pour intégrer les nouveaux membres de l'équipe et garantir une intégration continue (DevSecOps)
- L'IA est un outil indispensable pour améliorer la sécurité mais requiert des compétences spécifiques
  - ➢ **IL N'EXISTE PAS DE BAGUETTE MAGIQUE !**