



**MINISTÈRE
DE LA JUSTICE**

*Liberté
Égalité
Fraternité*

**Examen professionnel pour l'accès au troisième grade de secrétaire administratif du
ministère de la justice au titre de 2025**

Épreuve écrite d'admissibilité du 11/02/2025

L'épreuve écrite d'admissibilité consiste en la rédaction, à partir d'éléments d'un dossier portant sur des thèmes en relation avec les activités du ministère de la justice, d'une note administrative ou d'un rapport permettant de vérifier des capacités de compréhension et à rédiger clairement et correctement.

Durée de l'épreuve : 3 heures.

EMPLOYEZ EXCLUSIVEMENT DE L'ENCRE FONCÉE : NOIRE ou BLEUE et évitez toute présentation pouvant constituer un signe distinctif : cela entraînerait la non-correction de la copie et l'annulation de votre participation.

Sur la bande d'anonymat de chacune de vos copies :

Inscrivez vos nom, prénom, numéro d'inscription, date de naissance.

L'absence de ces mentions sur un feuillet entraînera la non-correction de votre copie et l'annulation de votre participation.

Numérotez chacune de vos pages dans la partie réservée en bas de chaque page.

Ne pas rabattre le haut de la copie.

Sur votre copie :

Ne faites apparaître aucun signe distinctif en quelque endroit de votre composition : cela entraînerait la non-correction de votre copie et l'annulation de votre participation.

À l'issue de l'épreuve :

Rendez votre copie même si elle est vierge, avec toutes les bandes d'anonymat renseignées, avant de signer la feuille d'émargement. Tout candidat quittant la salle sans rendre sa copie est signalé absent.

Aucun brouillon ni feuille non réglementaire ne sont acceptés.

La qualité de la rédaction, la clarté et la précision des raisonnements entrent pour une part importante dans l'appréciation du candidat.

L'usage de la calculatrice n'est pas autorisé.

SIGNES DISTINCTIFS ET ANONYMAT

Toute copie en rupture d'anonymat ou comportant des signes distinctifs entraînera l'élimination du candidat concerné par les membres du jury.

Sera considéré comme une rupture d'anonymat tout élément apparent sur la ou les copies remises et permettant d'identifier le candidat (nom, prénom, date de naissance, numéro de convocation, signature).

Les noms fictifs, initiales, noms de la commune de résidence du candidat, lieu de la salle d'examen seront également considérés comme signes distinctifs.

Les candidats doivent écrire et, le cas échéant souligner, au stylo bille, de couleur noire ou bleue uniquement. Une autre couleur pourrait être considérée comme un signe distinctif par le jury.

L'utilisation de plus d'une couleur (noire ou bleue) dans une même copie sera considérée comme signe distinctif. Le candidat est entièrement responsable de la copie qu'il remet après avoir fini l'épreuve.

Lors de la remise des copies et afin de respecter une stricte égalité de traitement des candidats :

- aucun rappel des consignes ne sera fait, même s'il est constaté des copies non conformes (en rupture d'anonymat ou avec signes distinctifs),
- ni les surveillants, ni le responsable de la salle, de hall ou de site ne se substitueront au candidat pour vérifier la conformité des copies remises.



MINISTÈRE DE LA JUSTICE

*Liberté
Égalité
Fraternité*

Sujet :

Vous êtes secrétaire administratif à la Cour d'appel de XYZ. Votre chef de service doit intervenir lors d'une présentation ayant pour thème la gestion du risque numérique.

En vous appuyant sur les documents joints, il vous demande de rédiger à son intention une note présentant la gouvernance de la sécurité numérique de l'Etat et la déclinaison qui en est faite au ministère de la justice. Cette note explicitera par ailleurs la notion de risque numérique ainsi que les dispositions qu'il convient de prendre ou de respecter pour assurer la sécurité numérique.

Documents (29 pages) :

Document 1 : Arrêté du 17 février 2020 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de la justice (2 pages)

Document 2 : Arrêté du 26 juillet 2023 portant approbation de la politique ministérielle de sécurité numérique du ministère de la justice (1 page)

Document 3 : Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics – extrait (3 pages)

Document 4 : Politique Ministérielle de Sécurité Numérique – Extraits (4 pages)

Document 5 : « Nos missions », document de l'ANSII (1 page)

Document 6 : Cadre de gouvernance de la sécurité numérique de l'Etat (PSSIE) (2 pages)

Document 7 : « Le ministère de la Justice crée une direction du numérique », article Intranet du 30 janvier 2024 (1 page)

Document 8 : « Les 10 règles de base pour la sécurité numérique », article de Cyber.gouv.fr du 4 juin 2019 (3 pages)

Document 9 : « La sécurité des usages pro-perso », fiche de Cybermalveillance.gouv.fr (2 pages)



**MINISTÈRE
DE LA JUSTICE**

*Liberté
Égalité
Fraternité*

Document 10 : « La sécurité numérique », article intranet de novembre 2022 (2 pages)

Document 11 : Lettre cyber avril-mail 2024, fiche du secrétariat général (3 pages)

Document 12 : « Les risques liés au numérique tendent à se diversifier », article GPOMAG.fr du 13 mars 2022 (3 pages)

Document 13 : « Cybersécurité : le défi de la formation des dirigeants public », article publié dans la Gazette des Communes le 06/12/2023 (2 pages)

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE LA JUSTICE

Arrêté du 17 février 2020 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de la justice

NOR : JUST2003327A

La garde des sceaux, ministre de la justice,

Vu le code de défense, notamment ses articles L. 1141-1, R. 1143-1 (3°) et R. 1143-5 (8°) ;

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 modifiée relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment son article 9 ;

Vu le décret n° 2010-112 du 2 février 2010 modifié pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment ses articles 2, 22 et 23 ;

Vu l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale ;

Vu l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques ;

Vu l'arrêté du 18 août 2016 portant approbation de la politique ministérielle de défense et de sécurité pour le ministère de la justice ;

Vu l'instruction interministérielle n° 920 /SGDSN/ DCSSI du 12 janvier 2005 relative aux systèmes traitant des informations classifiées de défense de niveau Confidentiel défense ;

Vu l'instruction interministérielle n° 901 SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'information sensibles ;

Vu la circulaire n° 5725/SG du 17 juillet 2014 relative à la politique de sécurité des systèmes d'information de l'Etat,

Arrête :

Art. 1^{er}. – Sont désignés autorités qualifiées pour la sécurité des systèmes d'information (AQSSI), pour les directions et services placés sous l'autorité du ministre :

- pour le secrétariat général : le secrétaire général du ministère de la justice ;
- pour les directions placées sous l'autorité directe du ministre : le directeur ;
- pour l'inspection générale de la justice : l'inspecteur général, chef de l'inspection générale ;
- pour le Conseil d'Etat : le secrétaire général du Conseil d'Etat ;
- pour les services à compétence nationale rattachés directement au ministre ou à caractère interministériel : le directeur ou le chef de service.

Art. 2. – Sont désignés autorités qualifiées pour la sécurité des systèmes d'information (AQSSI) pour les établissements publics nationaux placés sous la tutelle du ministre et les autorités relevant du périmètre du ministère de la justice :

- les responsables, quel que soit leur titre, des fonctions de direction générale des établissements publics ;
- les responsables, quel que soit leur titre, des fonctions de direction générale des autorités administratives indépendantes et des autorités publiques indépendantes.

Art. 3. – L'autorité qualifiée est responsable de la sécurité des systèmes d'information au sein de sa direction, du service, de l'établissement ou de l'autorité. Sa responsabilité ne peut être déléguée.

Elle s'assure, à ce titre, de l'application des instructions ministérielles données en cette matière, sous l'autorité du haut fonctionnaire de défense et de sécurité.

Dans ce cadre, en liaison avec le haut fonctionnaire de défense et de sécurité (HFDS) et le fonctionnaire de sécurité des systèmes d'information (FSSI) qui lui est rattaché, l'autorité qualifiée est chargée :

- de définir, à partir des objectifs de sécurité qu'il fixe, ou, pour les systèmes traitant d'informations classifiées, des objectifs de sécurité fixés par la présente instruction, une politique de sécurité des systèmes d'information adaptée à son service, sa direction, son établissement ou son organisme ;
- de désigner les autorités d'homologation des systèmes relevant de sa responsabilité ;
- de s'assurer que les dispositions réglementaires et, le cas échéant, contractuelles sur la sécurité des systèmes d'information sont appliquées, notamment celles relatives à la sécurité des systèmes traitant d'informations classifiées ;
- de faire appliquer les consignes et les directives internes ;
- de disposer d'une analyse, régulièrement mise à jour, des risques encourus par les SI de sa structure ;
- de s'assurer que des contrôles internes de sécurité sont régulièrement effectués ;
- d'organiser la sensibilisation et la formation du personnel aux questions de sécurité, en particulier en matière de systèmes d'information ;
- de s'assurer de la mise en œuvre des procédures réglementaires prescrites pour l'homologation des systèmes, pour l'agrément des dispositifs de sécurité et pour la gestion des articles contrôlés de la sécurité des systèmes d'information (ACSSI) ;
- de désigner les autorités d'homologation des systèmes et des services numériques relevant de sa responsabilité.

Art. 4. – Le présent arrêté sera publié au *Journal officiel* de la République française.

Fait le 17 février 2020.

NICOLE BELLOUBET

Document 2

RÉPUBLIQUE FRANÇAISE

Ministère de la justice

Arrêté du 26 JUIL. 2023
portant approbation de la politique ministérielle de sécurité numérique du ministère de la justice

NOR : JUST2321059A

Le garde des sceaux, ministre de la justice,

Vu le décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics ;

Vu l'arrêté du 17 février 2020 portant désignation des autorités qualifiées pour la sécurité des systèmes d'information dans les services d'administration centrale, les services déconcentrés, les organismes et établissements sous tutelle du ministre de la justice ;

Vu l'arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics,

Arrête :

Article 1^{er}

La politique ministérielle de sécurité numérique sur l'organisation de la sécurité numérique du système d'information et de communication du ministère de la justice et de ses établissements publics annexée au présent arrêté est approuvée.

Article 2

Les autorités qualifiées pour la sécurité des systèmes d'information (AQSSI) désigné aux articles 1 et 2 de l'arrêté du 17 février 2020 susvisé sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté.

Article 3

Le présent arrêté sera publié au Bulletin officiel du ministère de la justice.

Fait le **26 JUIL. 2023**

Pour le ministre et par délégation :
La secrétaire générale, haute fonctionnaire de défense et de sécurité,



C. CHEVRIER

Document 3

Arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics

NOR : PRMD2221955A

ELI : <https://www.legifrance.gouv.fr/eli/arrete/2022/10/26/PRMD2221955A/jo/texte>

[JORF n°0253 du 30 octobre 2022](#)

La Première ministre,

Vu le [code de la défense](#), notamment ses articles L. 1111-3, R.* 1132-1 à D. 1132-54 et R. 1143-1 à D. 1143-13 ;

Vu le [décret n° 87-389 du 15 juin 1987](#) modifié relatif à l'organisation des services d'administration centrale, notamment ses articles 3-5 et 3-8 ;

Vu le [décret n° 2009-834 du 7 juillet 2009](#) modifié portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information » ;

Vu le [décret n° 2019-1088 du 25 octobre 2019](#) modifié relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique ;

Vu le [décret n° 2022-513 du 8 avril 2022](#) relatif à la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics,

Arrêtent :

- [Article 1](#)

L'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'Etat et de ses établissements publics annexée au présent arrêté est approuvée.

- [Article 2](#)

Le ministre de l'économie, des finances et de la souveraineté industrielle et numérique, le ministre de l'intérieur et des outre-mer, la ministre de l'Europe et des affaires étrangères, le garde des sceaux, ministre de la justice, le ministre des armées, le ministre du travail, du plein emploi et de l'insertion, le ministre de l'éducation nationale et de la jeunesse, la ministre de l'enseignement supérieur et de la recherche, le ministre de l'agriculture et de la souveraineté alimentaire, le ministre de la transition écologique et de la cohésion des territoires, la ministre de la transition énergétique, la ministre de la culture, le ministre de la santé et de la prévention, le ministre des solidarités, de l'autonomie et des personnes handicapées, le ministre de la transformation et de la fonction publiques et la ministre des sports et des jeux Olympiques et Paralympiques sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté, qui entrera en vigueur le premier jour du sixième mois suivant celui de sa publication au Journal officiel de la République française.

ANNEXE

INSTRUCTION GÉNÉRALE INTERMINISTÉRIELLE NO 1337/SGDSN/ANSSI SUR L'ORGANISATION DE LA SÉCURITÉ NUMÉRIQUE DU SYSTÈME D'INFORMATION ET DE COMMUNICATION DE L'ÉTAT ET DE SES ÉTABLISSEMENTS PUBLICS

1. Introduction

En s'inscrivant pleinement dans la dynamique de la transformation numérique, les ministères et les établissements publics investissent largement le domaine du numérique. Ainsi, le système d'information et de communication de l'Etat devient désormais essentiel pour l'accomplissement des missions de ces administrations. Dans cette perspective, il importe que l'amélioration de la relation entre le public et l'administration qu'apporte le numérique ne soit pas sapée par une dégradation de la confiance des usagers dans ce système d'information et de communication.

Or, l'actualité montre que le développement du numérique est aussi générateur d'opportunités et de développements pour des attaquants aux profils et aux objectifs très variés. Au moment de la rédaction de cette instruction, la tendance est à la généralisation des menaces de masse telles que les rançongiciels aux conséquences significatives pour les administrations.

Compte tenu de ces menaces, la sécurité numérique, composante essentielle de la confiance numérique, ne doit plus être un domaine réservé aux seuls spécialistes. Le risque associé aux cyberattaques, s'il a ses spécificités, ne doit plus être traité de manière singulière. Il devient impératif que chaque direction d'administration, jusqu'au plus haut niveau hiérarchique, appréhende le risque numérique au même titre que les autres risques afin d'y consacrer les ressources humaines, budgétaires et techniques suffisantes pour le couvrir.

Cette prise en compte doit s'effectuer dans l'ensemble des missions de ces administrations mais également dans la définition d'une organisation de la gouvernance de la sécurité numérique, se déclinant à tous les échelons de l'Etat. La présente instruction définit l'organisation ainsi que les instances de la gouvernance de la sécurité numérique au niveau interministériel, dans les ministères, ainsi que dans les établissements publics d'Etat. Cette organisation conforte celle déjà définie dans la réglementation relative à la sécurité numérique en vigueur - notamment au travers de la protection du secret de la défense nationale avec l'instruction générale interministérielle 1300 - et l'étend pour permettre, notamment, l'appropriation du champ de la sécurité numérique par les chaînes métier. Elle porte également l'objectif de permettre une action coordonnée entre les acteurs du numérique, ceux de la sécurité numérique, de la protection des données à

caractère personnel et de la protection du secret de la défense nationale. Cet objectif se traduit aussi par la compatibilité entre les trois gouvernances respectives, afin de permettre une articulation efficace entre celles-ci et un niveau de synergie suffisant.

Afin de permettre aux ministères de mettre en œuvre cette organisation et ces instances tout en tenant compte de leurs particularités et de l'organisation existante, il est demandé à ces derniers de décliner l'organisation prévue par la présente instruction en s'appuyant sur l'existant autant que possible et en la précisant le cas échéant.

La première section de la présente instruction décrit les rôles et responsabilités associés à la gouvernance de la sécurité numérique au niveau interministériel. Cette section présente également les instances interministérielles de gouvernance de la sécurité numérique.

La deuxième section décrit les rôles et responsabilités associés à la gouvernance de la sécurité numérique dans les ministères. Cette section présente également les instances ministérielles de gouvernance de la sécurité numérique.

La troisième et dernière section décrit les rôles et responsabilités associés à la gouvernance de la sécurité numérique dans les établissements publics de l'Etat.

2. Champ d'application

L'application de la présente instruction est obligatoire pour les ministères et les établissements publics de l'Etat, quel que soit leur régime, ci-après nommés « établissements ». Les principes énoncés doivent être déclinés dans des instructions ministérielles en précisant les rôles et responsabilités au niveau ministériel.

L'application de l'organisation décrite dans le chapitre 5 de cette organisation est recommandée pour tous les autres organismes publics.

L'application de la présente instruction est sans préjudice de l'application de réglementations spécifiques, notamment celles relatives à la protection du secret de la défense nationale et à la protection des données à caractère personnel.

3. Organisation interministérielle de la gouvernance de la sécurité numérique de l'Etat

3.1. Vue d'ensemble de l'organisation interministérielle

3.1.1. Rappel de l'organisation de niveau étatique en matière de numérique

L'Etat se dote d'une stratégie du numérique de l'Etat qui vise à orienter les actions des administrations de l'Etat pour améliorer les services rendus par le système d'information et de communication de l'Etat. Le ministère de la transformation et de la fonction publique promeut les actions propres à accélérer la transformation numérique de l'Etat. La stratégie numérique de l'Etat est élaborée par le directeur interministériel du numérique sous l'autorité de son ministre de tutelle et approuvée par le Premier ministre. Le directeur interministériel du numérique pilote sa mise en œuvre, en liaison avec les directions du numérique des ministères.

3.1.2. Organisation étatique en matière de sécurité numérique

A travers la présente instruction, l'Etat se dote d'une politique de sécurité numérique de l'Etat.

Cette politique est complétée par les orientations stratégiques de sécurité numérique et la feuille de route associée, définies dans le comité stratégique interministériel de la sécurité numérique et validées en instance stratégique de niveau politique (cf. 3.3.1).

Les rôles et responsabilités contribuant particulièrement à la sécurité numérique au niveau interministériel, ainsi que les instances de gouvernance permettant de définir la stratégie interministérielle de sécurité numérique et d'assurer le suivi de sa mise en œuvre, sont décrits ci-après.

3.2. Rôles et responsabilités

3.2.1. Le Premier ministre

Le Premier ministre, en tant que responsable du système d'information et de communication de l'Etat, définit la politique de sécurité numérique de l'Etat. A ce titre, il valide l'organisation et les principes de la sécurité numérique du système d'information et de communication de l'Etat.

Le Premier ministre est assisté, dans l'exercice de ses responsabilités en matière de défense et de sécurité nationale, par le secrétaire général de la défense et de la sécurité nationale qui propose et met en œuvre la politique du gouvernement en matière de sécurité numérique. Il dispose à cette fin de l'Agence nationale de la sécurité des systèmes d'information.

3.2.2. L'Agence nationale de la sécurité des systèmes d'information (ANSSI)

L'Agence nationale de la sécurité des systèmes d'information assiste le secrétaire général de la défense et de la sécurité nationale pour la mise en œuvre de la politique de sécurité numérique de l'Etat. L'Agence nationale de la sécurité des systèmes d'information accompagne la direction interministérielle du numérique et les ministères dans l'articulation de cette politique avec leurs missions et en contrôle l'application.

L'Agence nationale de la sécurité des systèmes d'information anime et coordonne les travaux interministériels en matière de sécurité numérique. Elle élabore les mesures de sécurité des systèmes d'information et de communication proposées au Premier ministre et veille à leur application.

En lien avec chacun des ministères, l'Agence nationale de la sécurité des systèmes d'information réalise, selon une programmation annuelle, des audits et des inspections. Elle rend compte de cette mise en œuvre en comité stratégique

interministériel de la sécurité numérique.

L'Agence nationale de la sécurité des systèmes d'information, à travers son centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR), diffuse les informations relatives aux vulnérabilités des systèmes d'information et de communication et aux menaces. Ce centre est également le point de contact unique de signalement des incidents de sécurité.

L'Agence nationale de la sécurité des systèmes d'information maintient à jour un catalogue des services qu'elle propose aux administrations de l'Etat pour les accompagner dans leurs missions relatives à la sécurité numérique.

L'Agence nationale de la sécurité des systèmes d'information coordonne la réponse aux crises affectant la sécurité numérique de l'Etat selon l'organisation présentée en section 3.4.

Une convention entre l'Agence nationale de la sécurité des systèmes d'information et chaque ministère précise les relations entre les parties et décrit les services auxquels recourent les ministères ainsi que les modalités et responsabilités associées.

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information est membre du comité stratégique interministériel de la sécurité numérique (cf. 3.3.2).

Il préside le comité interministériel de pilotage de la sécurité numérique (cf. 3.3.3). L'Agence nationale de la sécurité des systèmes d'information assure le secrétariat de ce comité.

3.2.3. Le directeur interministériel du numérique (DINUM)

La direction interministérielle du numérique propose au Premier ministre et met en œuvre la stratégie numérique de l'Etat. Elle s'assure de la bonne prise en compte de la politique de sécurité numérique de l'Etat dans cette stratégie ainsi que dans les différents projets qui lui sont soumis au titre de cette stratégie et de ses attributions.

Pour les sujets relatifs à la sécurité numérique des services interministériels dont elle a la charge, la direction interministérielle du numérique s'inscrit dans la chaîne fonctionnelle de sécurité des systèmes d'information des services du Premier ministre.

Le directeur interministériel du numérique est autorité qualifiée en sécurité des systèmes d'information des systèmes d'information et de communication transverses dont il a la responsabilité. A ce titre, il assume les responsabilités décrites au 4.2.3.

La direction interministérielle du numérique établit et maintient à jour un catalogue des services qu'elle propose et le communique aux administrations de l'Etat afin de les accompagner dans leurs projets de transformation numérique. Pour chaque service, ce catalogue précise le niveau de sécurité numérique, le périmètre et les conditions d'emploi validés par l'autorité d'homologation.

Le directeur interministériel du numérique est membre du comité stratégique interministériel de la sécurité numérique (cf. 3.3.2). [...]

Fait le 26 octobre 2022.

La Première ministre,
Pour la Première ministre et par
délégation :
La secrétaire générale du Gouvernement,
Claire Landais

Le ministre de l'économie, des finances et
de la souveraineté industrielle et
numérique,
Bruno Le Maire

Le ministre de l'intérieur et des outre-mer,
Gérald Darmanin

La ministre de l'Europe et des affaires
étrangères,
Catherine Colonna

Le garde des sceaux, ministre de la justice,
Éric Dupond-Moretti

Le ministre des armées,
Sébastien Lecornu

Le ministre du travail, du plein emploi et
de l'insertion,
Olivier Dussopt

Le ministre de l'éducation nationale et de
la jeunesse,
Pap Ndiaye

La ministre de l'enseignement supérieur et
de la recherche,
Sylvie Retailleau

Le ministre de l'agriculture et de la
souveraineté alimentaire,
Marc Fesneau

Le ministre de la transition écologique et
de la cohésion des territoires,
Christophe Béchu

La ministre de la transition énergétique,
Agnès Pannier-Runacher

La ministre de la culture,
Rima Abdul-Malak

Le ministre de la santé et de la prévention,
François Braun

Le ministre des solidarités, de l'autonomie
et des personnes handicapées,
Jean-Christophe Combe

Le ministre de la transformation et de la
fonction publiques,
Stanislas Guerini

La ministre des sports et des jeux
Olympiques et Paralympiques,
Amélie Oudéa-Castéra

Politique Ministérielle de Sécurité Numérique

Version 2023-2024

1. Avant-propos

La transformation numérique, dans laquelle le ministère de la Justice est pleinement impliqué, accroît notre exposition au numérique. Dans un contexte où les menaces cyber sont protéiformes et en augmentation constante, les institutions publiques sont des cibles particulièrement exposées. Les menaces s'affranchissent des frontières, profitent des interdépendances des systèmes d'information et sont susceptibles d'impacter toute une institution.

Aussi, la sécurité numérique est une condition fondamentale pour répondre aux enjeux de la transformation numérique et des missions du service public de la Justice.

L'État répond à l'évolution des menaces et aux enjeux. Il déploie un dispositif d'ensemble qui se traduit notamment par une organisation de la gouvernance de la sécurité numérique, de la maîtrise du risque numérique et de la gestion des incidents de sécurité.

La présente politique ministérielle de sécurité du numérique décline pour le ministère de la Justice les moyens mis en œuvre dans ce domaine.

2. Champ d'application

2.1. Cadre légal

Le présent document définit la politique ministérielle de sécurité numérique du ministère de la justice (PMSN-MJ).

La PMSN vient décliner l'instruction générale interministérielle (IGI) n°1337/SGDSN/ANSSI du 26 octobre 2022 portant sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics. Cette politique prend en compte les spécificités du ministère de la justice et son organisation.

La PMSN s'adresse à l'ensemble des services du ministère et des établissements publics placés sous sa tutelle. La PMSN s'applique également, par voie contractuelle ou conventionnelle, aux gestions déléguées et aux services externalisés par le ministère de la justice (fournisseurs, prestataires de services, sous-traitants, etc.) ainsi qu'aux partenaires (organisations syndicales, mutuelles, associations, etc.) lorsqu'ils concourent aux missions du ministère ou qu'un accès aux informations du ministère leur a été accordé. L'ensemble de ces acteurs proches est appelé « écosystème numérique » du ministère de la Justice.

[...]

3. Organisation ministérielle de la gouvernance de la sécurité numérique

3.1. Chaînes, rôles et responsabilités

3.1.1. La chaîne décisionnelle de sécurité numérique

Afin de mener à bien ses missions, le garde des Sceaux, ministre de la justice, s'appuie sur une **chaîne décisionnelle** et sur des **instances de gouvernance** pour définir et contrôler la stratégie ministérielle de sécurité du numérique. Cette stratégie a pour objectif d'accompagner le plan de transformation numérique et de renforcer la résilience du ministère face aux cyberattaques.

Les rôles et responsabilités présentés ici sont issus de l'arrêté du 26 octobre 2022 portant approbation de l'instruction générale interministérielle n° 1337/SGDSN/ANSSI sur l'organisation de la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics. Cette section décline ces rôles dans le cadre du ministère de la Justice.

3.1.1.1. *Le garde des Sceaux, ministre de la Justice*

Le **garde des Sceaux est responsable de la sécurité numérique** des systèmes d'information et de communication du ministère et de ses établissements publics.

À ce titre, le ministre valide la politique ministérielle de sécurité numérique (PMSN), fixe les orientations stratégiques et s'assure que l'ensemble des systèmes d'information (SI) du ministère sont sous la responsabilité d'une autorité qualifiée en sécurité des SI (AQSSI) en charge de la **maîtrise des risques numériques**.

Le ministre **préside le comité stratégique de la sécurité numérique** pendant lequel la feuille de route et les amendements de la politique ministérielle de sécurité numérique sont approuvés.

3.1.1.2. *Le haut fonctionnaire de défense et de sécurité*

Le **haut-fonctionnaire de défense et de sécurité** (HFDS)(1) conseille le ministre pour toutes les questions relatives à la sécurité du numérique.

À ce titre, le HFDS **propose au ministre la politique ministérielle de sécurité numérique** qu'il est chargé d'animer.

[...]

Le HFDS **préside le comité de pilotage de sécurité numérique**. À ce titre, le HFDS planifie et anime ce comité. Il peut décider de déléguer cette présidence au fonctionnaire de sécurité des systèmes d'information (FSSI).

3.1.1.3. *Les autorités qualifiées en sécurité des systèmes d'information*

L'**autorité qualifiée en sécurité des systèmes d'information** (AQSSI) est responsable de la sécurité des services numériques placés sous sa responsabilité et de leur homologation. [...]

L'AQSSI réalise de plusieurs missions :

- Garantir les ressources nécessaires pour mener à bien les projets de transformation numérique de son périmètre et **s'assurer que les risques numériques sont connus et maîtrisés**.
- Réaliser et tenir à disposition du HFDS la **cartographie des risques numériques et des partenaires essentiels** à son activité.
- **Contribuer à l'élaboration du rapport annuel de sécurité numérique** qui intègre l'évaluation du niveau de risque de chaque direction et la synthèse des incidents de sécurité numérique pour le ministère. [...]
- **Participer à la résilience du ministère par l'élaboration et la mise en œuvre des plans de continuité d'activité** pour faire face à des incidents de sécurité numérique.

S'assurer au travers d'exercices de la connaissance, de la **maîtrise des plans de reprise et de continuité d'activité, et de leur mise à jour**. [...]

Sont désignés « autorités qualifiées en sécurité des systèmes d'information » :

- Les directeurs des administrations centrales,
- Les chefs de service à compétence nationale rattachés directement au ministre ou à caractère interministériel,

Les directeurs des établissements publics de l'État. [...]

3.1.1.4. *Le chef du service numérique (SNUM)*

Le **chef du service du numérique** ministériel (SNUM) définit la stratégie d'hébergement des services numériques et il s'assure de la prise en compte dans son service de la politique ministérielle de sécurité du numérique.

Le chef du SNUM assure la **mise en œuvre et l'exploitation de services numériques et d'infrastructures du ministère**.

A ce titre, pour les SI dont il a la charge, il veille :

- A l'élaboration et au maintien à jour d'une cartographie des systèmes d'information sous sa responsabilité ;
- Au maintien en condition opérationnelle et de sécurité des SI ;
- A la résilience numérique des services dont il a la charge ;
- A l'élaboration et la mise en œuvre des plans de continuité et de reprise informatique ;
- A la fourniture de moyens permettant de prévenir et de répondre aux incidents d'origine cyber. [...]

3.1.2. La chaîne fonctionnelle de sécurité numérique

[...] Cette chaîne a la charge du **pilotage et du contrôle de la mise en œuvre opérationnelle** de la stratégie de sécurité numérique. [...]

3.1.2.1. Le fonctionnaire de sécurité des systèmes d'information

Le **fonctionnaire de sécurité des systèmes d'information (FSSI)** pilote la mise en œuvre de la politique ministérielle permettant de maîtriser les risques de sécurité du numérique, de garantir la continuité des activités et la résilience du ministère.

Le **FSSI pilote la réponse aux incidents « très grave »**. À ce titre, il s'appuie sur le CSIRT ministériel placé sous son autorité.

Il informe l'agence nationale de sécurité des systèmes d'information (ANSSI) des incidents « grave » et « très grave » sur les systèmes d'information et de communication du ministère et des organismes placés sous sa tutelle.

3.1.2.2. Les conseillers à la sécurité du numérique (CSN)

Le **conseiller à la sécurité du numérique (CSN)** conseille et accompagne l'autorité qualifiée en sécurité des systèmes d'information dans l'exercice de ses responsabilités **pour la gestion des risques numériques**, les démarches d'homologation, l'évaluation fonctionnelle des incidents numériques, **l'anticipation et le traitement des crises d'origine cyber**. [...]

Sans être un expert technique du domaine, il dispose d'une culture de la sécurité du numérique qui lui permet de traduire les enjeux en exigences de sécurité pour le compte de l'AQSSI.

3.1.2.3. Les responsables centraux de la sécurité des systèmes d'information (RCSSI)

Les **responsables centraux de la sécurité des systèmes d'information (RCSSI)** sont les RSSI du **service numérique ministériel et des directions d'administration centrale**. [...]

3.1.3. La chaîne opérationnelle de sécurité numérique et de cyberdéfense

Pour mener à bien ses missions, le ministère s'appuie sur une **chaîne opérationnelle dédiée** et sur des **instances de suivi** qui permettent de décliner de manière concrète et pragmatique la stratégie ministérielle de sécurité numérique en recherchant l'efficacité.

3.1.3.1. Le responsable du CSIRT ministériel

Le **responsable du CSIRT ministériel** est en charge de la veille cyber, de la préparation et de la réalisation d'exercices cyber, et du pilotage et de la réponse sur incident numérique « grave » et « très grave ». Il assure la bonne exécution des investigations et de la coordination des parties prenantes permettant de garantir une réponse efficace. [...]

3.1.3.2. Le responsable SOC ministériel

Le **responsable du SOC ministériel** est responsable de la gestion technique des incidents de sécurité numérique. [...]

3.1.3.3. Les responsables de la sécurité des systèmes d'information (RSSI)

Les **responsables de la sécurité des systèmes d'information (RSSI)** sont des **experts techniques** qui peuvent être affectés auprès :

- D'un CSN pour l'appuyer dans les domaines techniques propres à sa direction métier.
- D'un service à compétence nationale afin de traiter les spécificités de l'entité. [...]
- D'une direction de programme afin de traiter les spécificités du projet. [...]
- D'une structure numérique afin de maintenir, superviser, contrôler les systèmes locaux, [...]

5. La gestion des incidents de sécurité

5.1. Définitions

Un **incident de sécurité** est un événement qui perturbe ou altère le fonctionnement d'un service et dont la gravité peut porter atteinte aux missions du ministère et au bon fonctionnement de la justice. En fonction du degré de gravité sur l'organisation, l'incident peut être catégorisé de « simple » à « très grave » et nécessiter l'activation d'une cellule de crise.

La gestion des incidents a pour but de qualifier et de neutraliser les effets des incidents pour rétablir le service le plus rapidement possible et s'assurer que l'incident ne se reproduise pas.

5.2. Catégorie et gestion des incidents de sécurité

Le ministère doit qualifier les incidents de sécurité par niveau de gravité qui est fonction de l'impact sur le fonctionnement des services :

- **Faible** : Les services sont légèrement perturbés (perceptible, localisé), mais sans réel impact pour les activités du ministère, le fonctionnement d'une structure ou d'un établissement.
- **Modéré** : Le fonctionnement d'un service est perturbé (constaté, gêne dans le fonctionnement), mais les impacts sont limités ou localisés. Ils ne portent pas atteinte de manière significative au bon fonctionnement de la structure ou de l'établissement.
- **Grave** : Les services sont perturbés au niveau national ou en ruptures au niveau local ou se propagent. Les structures locales rencontrent des difficultés sérieuses dans leur fonctionnement.
- **Très grave** : La conjonction de plusieurs incidents graves ou d'un incident majeur qui altère le fonctionnement des activités judiciaires, d'une zone de défense, d'un nombre important d'établissements, de l'ensemble des services d'une direction, d'un SIIV. [...]

5.3. Déclaration des incidents à la CNIL

Tout incident, quelle que soit la gravité, fait l'objet d'un signalement circonstancié et détaillé au délégué à la protection des données (DPD) du ministère. Ce signalement est initié par le responsable du CSIRT et complété par les CSN des entités impactées.

Seul le DPD et ses équipes sont en capacité d'estimer la nécessité de déclarer l'incident à la CNIL et d'opérer cette déclaration.

Document 5

Nos missions

Créée en 2009, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité et de cyberdéfense. Son action pour la protection de la Nation face aux cyberattaques se traduit en quatre grandes missions : défendre, connaître, partager, accompagner.

Source : ANSII - Publié le 04 Octobre 2023 Mis à jour le 06 Décembre 2023

Les technologies numériques sont aujourd'hui omniprésentes dans le fonctionnement de l'État, de l'activité des entreprises et dans la vie quotidienne de chaque citoyen. Qu'elles soient en cours ou à venir, ces transformations sont synonymes de formidables opportunités.

Mais plus notre société se numérise, plus elle s'expose aux risques inhérents à ces technologies. Les attaques informatiques sont désormais susceptibles de porter gravement atteinte au fonctionnement de la société, à l'économie et à la sécurité nationale.

Dans ce contexte, la raison d'être de l'ANSSI, agence interministérielle, est de construire et d'organiser la **protection de la Nation face aux cyberattaques**. Elle contribue ainsi à **renforcer le niveau de cybersécurité global et la stabilité du cyberespace**.

1. Défendre...

- ...les systèmes d'information critiques de la Nation en concevant et opérant le déploiement de capacités de détection des cyberattaques ;
- ...les victimes de cyberattaques d'ampleur ;
- ...la Nation en structurant au niveau national l'assistance aux victimes de cyberattaques.

2. Connaître...

- ...l'état de l'art en sécurité des technologies et des systèmes d'information et en être des experts ;
- ...les menaces et les risques dans le cyberespace et développer des méthodes et des outils pour y faire face ;
- ...les tendances du monde de la cybersécurité, en France, en Europe et à l'international, pour s'y inscrire pleinement en défendant une vision singulière de la sécurité et de la stabilité du cyberespace.

3. Partager...

- ... des recommandations de cybersécurité, des solutions et des outils aux acteurs de la cybersécurité et de la transformation numérique pour démultiplier l'action de l'agence et renforcer la cybersécurité collective ;
- ...sur la réponse à la menace au sein des réseaux de coopération techniques, opérationnels et stratégiques français, européens et internationaux ;
- ... l'expertise de l'agence dans le domaine de la cybersécurité pour former les agents de l'État et des opérateurs régulés à la cybersécurité ;
- ...largement les connaissances en matière de cybersécurité et encourager le développement de la filière et des formations en cybersécurité ;
- ..., en lien avec ses partenaires, pour informer et sensibiliser les citoyens aux risques cyber.

4. Accompagner...

- ...le développement d'une doctrine française de cybersécurité et la conception des dispositifs normatifs et réglementaires aux niveaux national et européen ;
- ...le Gouvernement dans le déploiement d'une politique publique en matière de cybersécurité ;
- ...les plus hautes autorités dans leur appréhension du fait cyber ;
- ...les opérateurs régulés dans l'application des mesures de sécurisation de leurs systèmes d'information et leurs réponses aux incidents ;
- ...le développement d'un écosystème de prestataires de produits et de services de confiance dans le domaine de la cybersécurité.

Document 6

Cadre de gouvernance de la sécurité numérique de l'État (PSSIE)

Source : ANSII Publié le 18 Août 2022 Mis à jour le 11 Octobre 2023

Le cadre de gouvernance de la sécurité numérique de l'État, corédigé avec l'ensemble des ministères, renforce la prise en compte du risque numérique dans la mise en œuvre et l'exploitation des systèmes d'information et de communication de l'État par les ministères et les établissements publics d'État.

Ce cadre vise à :

- Responsabiliser les dirigeants (par exemple les directeurs d'administration centrale ou les responsables d'établissement) à la sécurité numérique ;
- Renforcer la sécurité numérique des établissements publics de l'État ;
- Responsabiliser les acteurs de la transformation numérique ;
- Assurer la cohérence avec les principaux textes réglementaires définissant une gouvernance en matière de numérique ou de sécurité, notamment la nouvelle IGI 1300 et le décret n° 2019-1088 définissant les responsabilités de la direction interministérielle du numérique (DINUM) ;
- Assurer la gouvernance aux différents niveaux de l'État via la mise en place d'une procédure de prise de décision aux niveaux interministériel et ministériel.

Le cadre de gouvernance, à terme, se substituera à la circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 introduisant la politique de sécurité des systèmes d'information de l'État (PSSIE). Actuellement les deux cohabitent et se complètent, surtout en ce qui concerne les règles de sécurité prévues par cette PSSI.

Ce cadre s'articule autour :

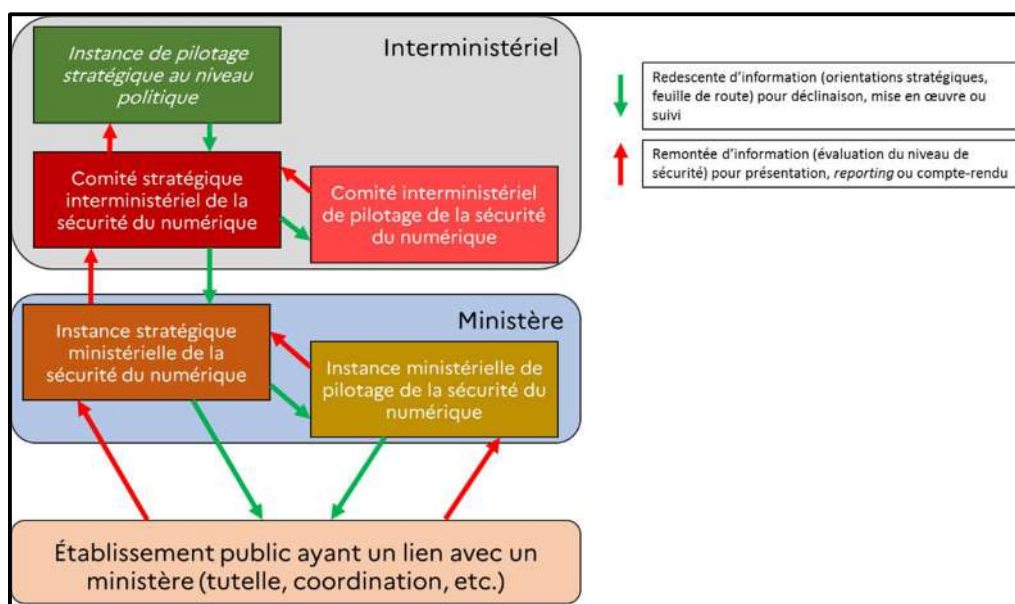
- Du décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'État et à la direction interministérielle du numérique modifié par le décret n° 2022-513 du 8 avril 2022 relatif à la sécurité numérique du système d'information et de communication de l'État et de ses établissements publics.
- De l'instruction générale interministérielle n°1337/SGDSN/ANSSI sur l'organisation de la gouvernance de la sécurité numérique de l'État, approuvée par arrêté.
- D'une instruction générale interministérielle qui portera les règles de sécurité numérique de l'État.
- La circulaire du Premier ministre n° 5725/SG du 17 juillet 2014 introduisant la politique de sécurité des systèmes d'information de l'État (PSSIE).

À qui s'adresse cette réglementation ?

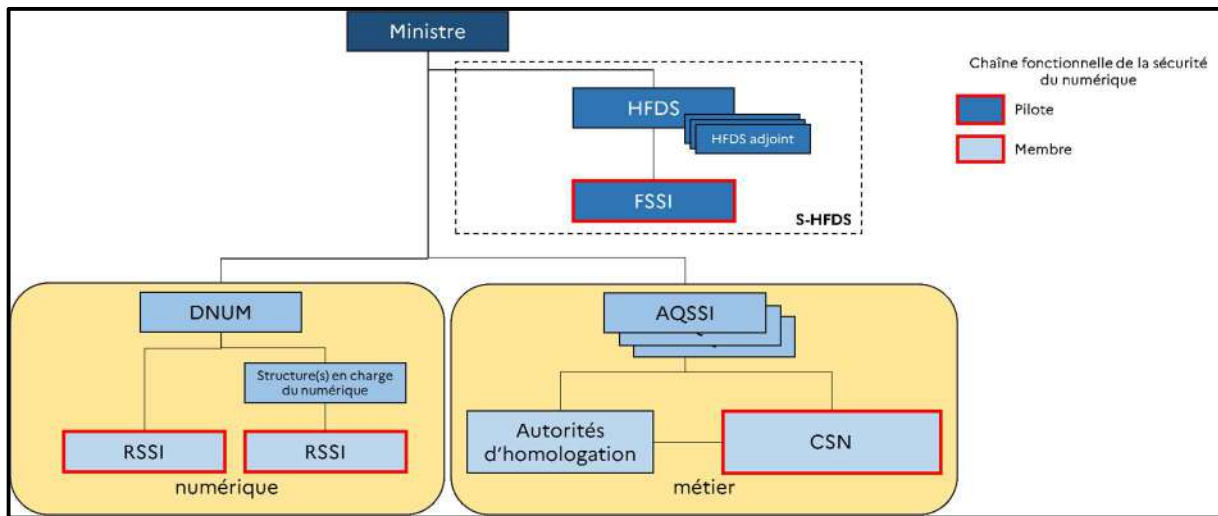
Cette réglementation s'applique aux ministères et aux établissements publics d'État sous la tutelle de ces derniers.

Que contient-elle ?

Le cadre de gouvernance de la sécurité numérique de l'État définit une comitologie permettant la prise en compte de la sécurité numérique aux niveaux interministériel et ministériel aux niveaux stratégique et opérationnel. Cette comitologie est présentée ci-dessous.



De plus, ce cadre de gouvernance en s'appuyant notamment sur l'organisation définie dans l'instruction générale interministérielle no 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale, définit les rôles et responsabilités pour une prise en compte de la sécurité numérique au bon niveau. L'organisation cible est présentée ci-dessous bien que chaque ministère, conserve un degré de liberté pour adapter cette organisation à son contexte et son organisation.



Enfin, le cadre de gouvernance de la sécurité numérique de l'État fait porter la responsabilité de la sécurité numérique des établissements publics d'État sur les dirigeants exécutifs de ces établissements qui doivent s'assurer de la conformité aux exigences suivantes :

- La définition et la mise en œuvre d'une organisation en matière de sécurité numérique ;
- La désignation et la communication à l'ANSSI des coordonnées d'un point de contact sur les sujets relatifs à la sécurité numérique ;
- La réalisation d'une évaluation annuelle du niveau de sécurité ;
- La notification des incidents de sécurité.

Quel est le rôle de l'ANSSI ?

En plus des missions qui lui ont été attribuées au titre du décret n° 2009-834 du 7 juillet 2009 modifié, le cadre de la gouvernance de la sécurité numérique de l'État confie à l'ANSSI les missions suivantes :

- La participation au comité stratégique interministériel de la sécurité numérique (COSINUS) afin de présenter un état de la menace en matière de sécurité numérique ;
- La présidence de l'instance interministérielle de pilotage de la sécurité numérique (CINUS) permettant de suivre la mise en œuvre de la feuille de route définie au niveau politico-stratégique et de partager et réfléchir sur les difficultés rencontrées par les différents participant ;
- La participation, sur invitation des ministères, à leur instance stratégique ministérielle de la sécurité numérique ;
- Le maintien à jour d'un catalogue des services qu'elle propose aux administrations de l'État et l'établissement d'une convention précisant, parmi ces services, ceux que l'ANSSI fournit au bénéfice de chaque ministère ;
- L'accompagnement des bénéficiaires dans leur mise en conformité avec ce nouveau cadre, notamment via la publication de guides ou la qualification de produits ou services de sécurité ;
- La réception et le traitement des incidents significatifs que les administrations de l'État et les établissements publics d'État pourraient lui notifier.

Document 7

Le ministère de la Justice crée une direction du numérique

Par décret n° 2024-46 du 29 janvier 2024, le garde des Sceaux a transformé le service du numérique en une direction du numérique (DNUM). La création de cette direction donne au numérique une place plus adaptée au sein de notre institution.

Source : Intranet ministère de la Justice

Pourquoi une direction ?

Le fonctionnement de la justice repose de façon croissante sur les outils numériques. Ce sont des leviers majeurs pour améliorer le quotidien des agents et des justiciables et atteindre les grands objectifs du ministère, **notamment en matière de réduction des délais.**

La création d'une direction permet de consacrer la place acquise par le numérique au sein de notre institution, et d'adopter une organisation qui est désormais celle de la plupart des grands ministères (Armées, Intérieur et Outre-mer, Transition écologique, Affaires sociales, Éducation).

La création de cette nouvelle direction est accompagnée de plusieurs évolutions dans la façon de piloter le numérique au ministère, qui permettront :

- Un renforcement du portage du numérique au sein des grandes directions (DAP, DSJ, DPJJ, DACS, DACG), des services du secrétariat général (SADJAV, SEM, SRH, DICOM...) et de l'ATIGIP, pour qu'ils l'utilisent de manière optimale comme un levier de réalisation des missions et de conduite des transformations qui leur sont confiées ;
- Une plus grande cohérence dans les chantiers numériques, destinée en particulier à mieux interconnecter les applications pour éviter les ressaisies, à renforcer la cohérence du soutien aux utilisateurs, et à remédier à l'obsolescence des outils ;
- Une amélioration de l'écoute et de la mesure de satisfaction des agents du ministère pour mieux les intégrer dans les évolutions techniques, de prioriser davantage la recherche de gains de temps et la résolution des « irritants » ressentis par les agents dans nos développements applicatifs ;
- Un pilotage plus fin de l'évolution des ressources humaines consacrées au numérique, en veillant à la montée en compétence des agents qui en ont besoin ;
- Une meilleure organisation des projets applicatifs, en favorisant notamment des projets intégrant maîtrise d'ouvrage et maîtrise d'œuvre au sein d'une même équipe, à l'image de la procédure pénale numérique (PPN). Ces directions de projets pourront être portées par les directions métier du ministère, qui bénéficieront ainsi de capacités renforcées d'atteindre leurs objectifs.

Quelle organisation ?

Comme l'était le service du numérique, **la DNUM reste au sein du secrétariat général, rattachée au secrétaire général adjoint en charge de la transformation numérique.**

La DNUM bénéficiera de **plusieurs emplois supplémentaires en 2024** qui permettront notamment de renforcer l'encadrement, de développer la fabrique numérique interne et son incubateur et de créer une animation et des offres de service dans le domaine des compétences numériques des agents, de l'écoute et l'association des utilisateurs. Elle sera renforcée avec la création d'une troisième sous-direction et d'une mission dédiée à l'amélioration de l'écoute et de l'association des utilisateurs, au développement des compétences numériques, et à l'amélioration des méthodes.

La DNUM poursuivra son rôle d'animation des DIT (départements informatique et télécommunications) rattachés aux délégués interrégionaux du secrétariat général.

Dans son rôle de maîtrise d'œuvre informatique, de coordination et de mise en cohérence, d'appui et de conseil et de partage de bonnes pratiques, **la DNUM intensifiera enfin ses partenariats avec les grandes directions métier du ministère** qui pilotent chacune un pan du système d'information du ministère.

Document 8

Les 10 règles de base pour la sécurité numérique

Publié le 04 juin 2019 - Modifié le 27 novembre 2024

Source : cyber.gouv.fr

De votre tablette à votre ordinateur, en passant par votre téléphone portable, êtes-vous vraiment attentif à votre sécurité numérique ?

Pour le savoir, découvrez **les 10 règles de base pour vous protéger sur Internet** :

1. Adopter une politique de mot de passe rigoureuse

C'est l'un des gestes les plus simples à mettre en œuvre, et pourtant beaucoup le négligent : à chaque nouvelle inscription sur un site web, il vous faut adopter une gestion de mot de passe solide.

Pour cela, voici quelques bonnes pratiques à avoir en tête :

- Utilisez un mot de passe différent pour chaque accès : c'est la première chose à faire pour limiter les dégâts éventuels en cas de piratage.
- Utilisez un mot de passe suffisamment long et complexe : au minimum 12 caractères contenant des minuscules, des majuscules, des chiffres et des caractères spéciaux.
- Dans le cadre de votre navigation personnelle, changez vos mots de passe au moindre doute d'utilisation frauduleuse.
- Dans le cadre professionnel, n'attendez pas de soupçonner une fraude et modifiez vos mots de passe de façon régulière et systématique.
- Utilisez un mot que personne ne peut deviner : personne ne doit pouvoir le reconstituer, pas même vos proches. Evitez donc toute information très facile d'accès comme votre date de naissance ou le nom de votre chien.
- Ne communiquez jamais votre mot de passe à un tiers : Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe. Si l'on vous demande votre mot de passe après avoir cliqué dans un courriel, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.
- Utilisez un gestionnaire de mots de passe : téléchargez un outil comme KeePass qui se chargera de mémoriser tous vos mots de passe et vous permettra de générer des mots de passes aléatoires suffisamment longs et complexes.
- Choisissez un mot de passe particulièrement robuste pour votre boîte de messagerie : l'adresse de messagerie est souvent demandée pour vous inscrire sur un site Internet. Sur cette adresse, vous pouvez recevoir les liens de réinitialisation des mots de passe des comptes en ligne sur lesquels vous êtes inscrits. Si un cybercriminel parvenait à pirater votre messagerie, il pourrait prendre le contrôle de tous vos comptes en ligne (réseaux sociaux, compte bancaire, sites administratifs, etc.).

2. Sauvegarder ses données régulièrement

Sauvegarder régulièrement vos données personnelles et professionnelles vous protège en cas de **panne**, de **perte**, de **vol**, de **destruction** de votre matériel ou de **piratage informatique**. Et pourtant, la majorité des internautes ne mettent en place une routine de sauvegarde régulière **qu'après** avoir subi une première perte de données... Pourquoi attendre d'en être victime alors que vous pouvez mettre en place cette routine dès aujourd'hui ?

Voici les différentes options qui s'offrent à vous pour sauvegarder vos données numériques :

Cas n°1 : Sauvegarder un volume de données faible

- Si vous souhaitez stocker un volume limité de données, **une clé USB voire un DVD enregistable** devraient suffire.
- Vous pouvez aussi opter pour **un service de stockage en ligne (cloud)**. Il existe des solutions gratuites ou payantes en fonction de la capacité de stockage souhaitée.

Cas 2 : Sauvegarder un volume de données conséquent

- Pour effectuer des sauvegardes de plus grande envergure, **le disque dur externe** est la meilleure option.
- Si vous manquez encore de place et que vous êtes à l'aise en informatique, vous pouvez également envisager le **stockage en réseau**. Créez votre propre serveur FTP ou bien achetez un Network Attached Storage (NAS) : vous pourrez alors partager des fichiers sur un serveur accueillant différents disques durs.

3. Sécurité numérique : faire ses mises à jour régulièrement

Un appareil ou un logiciel qui n'est pas à jour **est vulnérable et davantage susceptible de faire l'objet d'attaques informatiques**.

Voici quelques conseils pour ne plus s'exposer à ce risque :

- Identifiez l'ensemble de vos appareils et logiciels utilisés.
- Lorsque l'on vous propose une mise à jour, faites-la **immédiatement**.
- Téléchargez les mises à jour uniquement depuis les sites officiels des éditeurs.

- Sur vos appareils, activez **l'option de téléchargement et d'installation automatique des mises à jour** si elle existe.
- Anticipez vos périodes d'inactivité pour réaliser vos mises à jour lors de ces moments.
- Méfiez-vous de fausses mises à jour que l'on vous propose sur Internet. Restez extrêmement vigilant car il peut s'agir d'une technique pour vous inciter à installer une prétendue mise à jour qui serait en réalité un virus.

4. Se protéger des virus et autres logiciels malveillants

Sur Internet, **les fichiers malveillants** sont nombreux et variés.

Virus, vers, cheval de Troie, ou logiciels espions (spyware) sont tout autant de techniques couramment utilisées par les pirates informatiques. Pour vous protéger de ces intrusions, il est indispensable de posséder ces deux outils :

- **Un antivirus**
- **Un pare-feu bien configuré** qui bloquera les connexions non désirées depuis votre ordinateur
- Réalisez des analyses (ou scans) de votre ordinateur, votre téléphone mobile, votre tablette régulièrement pour identifier la présence de programmes malveillants. Lorsque votre antivirus demande à ce que ses bases virales soient mises à jour, faites-le immédiatement. De même, lorsqu'il vous signale un fichier suspect et vous propose de le supprimer ou de le mettre en quarantaine, réalisez l'opération au plus vite.

Par ailleurs, quelques bonnes pratiques sont de rigueur lorsque vous utilisez des appareils de stockage externe, comme des clés USB ou des disques durs externes :

- N'utilisez jamais un service ou un équipement inconnu ou abandonné.
- Attribuez un usage spécifique à chaque clé USB pour réduire les effets d'une éventuelle contamination.
- Chiffrez le contenu de vos appareils de stockage pour éviter le piratage.

5. Évitez les réseaux Wi-Fi publics ou inconnus

S'ils peuvent s'avérer très utiles, **les réseaux Wi-Fi publics sont une aubaine pour les pirates informatiques**. Très faciles d'accès, ces réseaux peuvent être contrôlés par des cybercriminels pour **intercepter vos informations personnelles**.

Voici quelques conseils pour éviter de vous connecter à ces réseaux ou, le cas échéant, vous en servir de façon sécurisée :

- Pour éviter que vos appareils ne se connectent automatiquement à ces réseaux, **désactivez les connexions sans-fil** (Wi-Fi, Bluetooth, NFC, ...) lorsque vous ne vous en servez pas.
- Quand vous le pouvez, **privilégiez la connexion privée 3G ou 4G** associée à votre abonnement mobile. Et n'oubliez pas de sécuriser le partage de connexion de vos appareils à l'aide d'un mot de passe : cela évitera que n'importe qui puisse accéder directement à vos données partagées !
- Si vous n'avez d'autre choix que d'utiliser un Wi-Fi public, veillez à ne jamais y réaliser d'opérations à caractère sensible (paiement par carte bancaire, déclaration d'impôts, renseignement d'informations confidentielles, etc.) et, si possible, utilisez un réseau privé virtuel (VPN).

6. Sécurité numérique : Bien séparer ses usages professionnels et personnels

Avec la multiplication des accès à Internet, vos informations personnelles comme professionnelles deviennent accessibles de n'importe où. Il devient en effet possible de :

- Consulter vos mails professionnels dans votre salon.
- Jeter un œil à vos réseaux sociaux pendant une pause-café au bureau.
- Relire un contrat important dans le train puis regarder une retransmission sportive.

Ainsi, avec Internet, **la frontière entre vie professionnelle et vie personnelle devient** de plus en plus poreuse. Pour sécuriser au mieux vos usages numériques dans ces différents environnements, commencez par utiliser **un mot de passe différent** pour chaque service professionnel et personnel auquel vous avez accès.

Distinguez également vos usages sur les réseaux sociaux :

- Évitez de partager des informations professionnelles sur vos réseaux sociaux personnels. Le partage et l'interprétation d'informations peuvent très vite nuire à votre entreprise.
- À l'inverse, vous ne souhaitez probablement pas que votre entreprise ait connaissance de tout ce que vous publiez dans votre cercle privé.

Il en va de même pour **les messageries électroniques et les services de stockage en ligne**. Ne mélangez pas vos messages et utilisez des services en ligne (cloud) distincts pour stocker vos données professionnelles et personnelles. Sans cela, vous risquez au mieux une erreur de destinataire, au pire, si vous êtes piraté, cela pourrait mettre en danger votre entreprise si un cybercriminel accédait à des messages professionnels confidentiels.

7. Éviter de naviguer sur des sites douteux ou illicites et être vigilant lors du téléchargement d'un fichier

De façon générale, évitez de vous rendre sur des sites douteux ou illicites. Certains sont susceptibles d'héberger des contrefaçons et **peuvent contenir des virus**. N'utilisez pas de plateformes non-officielles et ne téléchargez pas de fichiers provenant d'un site de téléchargement illégal : de nombreux fichiers sont infectés et peuvent contenir des virus et autres logiciels malveillants. Certains sites pornographiques sont également de véritables nids à virus, soyez vigilant.

Pour télécharger de nouvelles applications sur votre ordinateur, tablette ou smartphone, nous vous recommandons de **n'utiliser que les magasins officiels** ou encore le site de l'application elle-même.

8. Contrôler les permissions des comptes utilisateurs

Un même poste de travail, serveur ou logiciel peut être accessible par plusieurs utilisateurs, chacun disposant **d'un accès plus ou moins restreint selon son niveau de permission**.

Lorsqu'il vous revient d'ajouter des utilisateurs à un appareil ou service, et donc de choisir le niveau de permission à leur accorder, appliquez toujours **la règle du privilège minimum** : assurez-vous que chacun des utilisateurs ait uniquement les permissions dont il a besoin.

Ce principe simple limite les conséquences dommageables en cas d'attaque et augmente considérablement votre **sécurité numérique**.

Comment faire ?

- Par défaut, tous les utilisateurs d'un poste de travail ou d'un serveur doivent avoir un niveau d'accès au système d'exploitation et aux informations limité.
 - Ensuite, personnalisez au maximum les attributions et possibilités de chacun en fonction de ses besoins.
- Enfin, surveillez bien chaque compte et l'utilisation qui en est faite.

9. Sécurité numérique : Être vigilant sur les liens ou les pièces jointes contenus dans des messages électroniques

L'hameçonnage (ou *phishing* en anglais) désigne une technique frauduleuse qui consiste à usurper l'identité d'un organisme connu (banque, opérateurs, etc) ou d'un proche pour récupérer des informations confidentielles.

Voici quelques recommandations simples pour l'éviter :

- Ne communiquez pas d'informations personnelles ou professionnelles par messagerie ou par téléphone.
- En cas de réception d'un message contenant un lien, positionnez le curseur de la souris (**sans cliquer**) sur ce lien ou, sur votre téléphone mobile, faites un appui long sur ce lien, toujours sans cliquer, pour afficher l'adresse vers laquelle il pointe réellement.
- **Vérifiez bien l'adresse du site Internet** avant de renseigner des données. Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux.
- Si le site le permet, activez **la double authentification** pour sécuriser vos accès.
- Utilisez des mots de passe de différents et complexes pour chaque site et application.
- Saisissez directement dans votre navigateur l'adresse du site concerné.

En cas de doute, contactez directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu. Si vous avez communiqué des informations bancaires, faites opposition à vos moyens de paiement et déposez plainte.

10. Faire attention aux informations personnelles ou professionnelles que l'on diffuse sur Internet

De façon générale, chacun doit se sentir responsable de ce qu'il diffuse sur l'internet. Ne communiquez jamais d'informations sensibles sur des sites qui vous semblent insuffisamment protégés **et jamais lorsque la mention "Non sécurisé" apparaît à gauche de l'adresse du site Internet**.

De la même manière, faites attention à bien identifier les personnes avec qui vous parlez sur Internet. Si vous avez un doute sur une identité, à cause d'une façon d'écrire inhabituelle par exemple, **contactez cette personne via un autre moyen** avant de répondre à toute question.

Enfin soyez toujours vigilant : même vos amis ou contacts peuvent vous envoyer ou partager des contenus malveillants, de façon non intentionnelle.

Avec ces 10 règles de **sécurité numérique** en tête, vous voilà mieux protégé pour naviguer sereinement sur Internet !



LA SÉCURITÉ DES USAGES PRO-PERSO



La transformation numérique modifie en profondeur les usages et les comportements. Être connecté est devenu le quotidien. Le développement des technologies mobiles (PC portables, tablettes, smartphones) offre désormais la possibilité d'accéder, depuis presque n'importe où, à ses informations personnelles mais aussi à son système informatique professionnel: la frontière numérique entre la vie professionnelle et personnelle devient de plus en plus poreuse. Face à cette évolution, il est nécessaire d'adapter ses pratiques afin de protéger tant votre entreprise* ou votre organisation, que votre espace de vie privée. **Voici 10 bonnes pratiques à adopter pour la sécurité de vos usages pro-perso.**

1 UTILISEZ DES MOTS DE PASSE DIFFÉRENTS POUR TOUS LES SERVICES PROFESSIONNELS ET PERSONNELS AUXQUELS VOUS ACCÉDEZ

Si vous ne le faites pas et qu'un des services auquel vous accédez se fait pirater, le vol de votre mot de passe permettra à une personne malveillante d'accéder à tous vos autres services y compris les plus critiques (banque, messagerie, sites marchands, réseaux sociaux...). Si vous utilisez ce même mot de passe pour accéder au système informatique de votre entreprise, c'est elle que vous mettez aussi en péril, car un cybercriminel pourrait utiliser vos identifiants de connexion pour voler ou détruire des informations.

2 NE MÉLANGEZ PAS VOTRE MESSAGERIE PROFESSIONNELLE ET PERSONNELLE

Ce serait, en effet, le meilleur moyen de ne plus s'y retrouver et de commettre des erreurs, notamment des erreurs de destinataires. Celles-ci pourraient avoir pour conséquences de voir des informations confidentielles de votre entreprise vous échapper vers des contacts personnels qui pourraient en faire un mauvais usage, ou à l'inverse de voir un message trop personnel circuler dans votre environnement professionnel alors que vous ne le souhaiteriez pas. Enfin,

comme votre messagerie personnelle est généralement bien moins sécurisée que votre messagerie professionnelle, vous faire pirater votre compte pourrait mettre en danger votre entreprise si un cybercriminel accédait à des messages professionnels confidentiels que vous auriez gardés dans votre messagerie personnelle.

3 AYEZ UNE UTILISATION RESPONSABLE D'INTERNET AU TRAVAIL

Si l'utilisation d'une connexion Internet professionnelle à des fins personnelles est tolérée, il est important d'avoir à l'esprit que votre utilisation peut mettre en cause votre entreprise qui pourra se retourner contre vous si vous commettez des actes répréhensibles comme du téléchargement illégal, de l'atteinte au droit d'auteur ou si vous publiez des propos qui pourraient être condamnables. De plus, vous devez avoir à l'esprit que votre entreprise est

en droit de contrôler votre utilisation de la connexion qu'elle met à votre disposition. N'utilisez donc pas votre connexion professionnelle pour des choses qui n'ont, selon vous, pas à être connues de votre entreprise.

4 MAÎTRISEZ VOS PROPOS SUR LES RÉSEAUX SOCIAUX

Quand vous parlez de votre travail ou de la vie de votre entreprise (ambiance, nouveaux projets...) sur les réseaux sociaux, même si vos propos ne sont pas négatifs, vous ne contrôlez pas vos lecteurs: la rediffusion ou l'interprétation qu'ils peuvent faire de vos informations pourraient nuire à votre entreprise. À l'inverse, et pour les mêmes raisons, vous n'avez pas forcément envie que certains propos que vous pouvez tenir sur les réseaux sociaux et qui concernent votre vie privée puissent être connus de votre entreprise. Sur les réseaux sociaux, verrouillez votre profil pour que tout ne soit pas public et avant de poster, demandez-vous toujours si ce que vous communiquez ne pourra pas vous porter préjudice, ou à votre entreprise, si d'aventure vos propos ou messages étaient relayés par une personne malintentionnée.



*Le terme « entreprise » employé dans ce document regroupera toutes les organisations professionnelles qu'elles soient à caractère privé, public ou associatif.

EN PARTENARIAT AVEC:

MINISTÈRE DE L'INTÉRIEUR

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION



5 N'UTILISEZ PAS DE SERVICES DE STOCKAGE EN LIGNE PERSONNEL À DES FINS PROFESSIONNELLES

Ou du moins pas sans l'autorisation de votre employeur et sans avoir pris les mesures de sécurité qui s'imposent. Ces services de stockage en ligne d'informations (*Cloud* en anglais) généralement gratuits pour les particuliers sont certes pratiques, mais d'un niveau de sécurité qui ne se prête pas forcément aux exigences des entreprises pour protéger leurs informations. Ils ne sont pas conçus pour cela. Pour les besoins des entreprises, il existe des solutions professionnelles et sécurisées. L'utilisation d'un service de stockage en ligne personnel pour des usages professionnels pourrait mettre en danger votre entreprise si votre compte d'accès à ce service était piraté alors qu'il contenait des informations confidentielles.

6 FAITES LES MISES À JOUR DE SÉCURITÉ DE VOS ÉQUIPEMENTS

Sur vos moyens informatiques personnels (ordinateur, téléphone, tablette), mais également sur vos moyens professionnels si cela relève de votre responsabilité, il est important d'installer sans tarder les misés à jour dès qu'elles

sont publiées. Elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations ou à celles de votre entreprise.

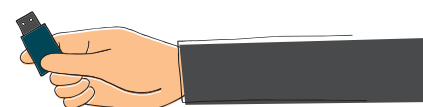
7 UTILISEZ UNE SOLUTION DE SÉCURITÉ CONTRE LES VIRUS ET AUTRES ATTAQUES

Sur vos moyens informatiques personnels (ordinateur, téléphone, tablette), mais également sur vos moyens professionnels si cela relève de votre responsabilité, utilisez une solution anti-virus et tenez-la à jour. Même si aucune solution n'est totalement infaillible, de nombreux produits peuvent vous aider à vous protéger des différentes attaques que peuvent subir vos équipements comme les virus, les rançongiciels (*ransomware*), l'hameçonnage (*phishing*)... Si un cybercriminel prenait le contrôle de vos équipements personnels, il pourrait accéder à toutes vos informations, mais aussi au réseau de votre entreprise si vous vous y connectez avec ce matériel.

8 N'INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OU MAGASINS OFFICIELS

Que ce soit pour vos usages personnels ou professionnels si cela relève de votre responsabilité, et même s'ils ne sont pas infaillibles, seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées par un virus qui permettrait à un cybercriminel de prendre le contrôle de votre équipement. Méfiez-vous des

sites « parallèles » qui ne contrôlent pas les applications qu'ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal : elles sont généralement piégées. Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d'installer une nouvelle application. Au moindre doute, ne l'installez pas et choisissez-en une autre.



9 MÉFIEZ-VOUS DES SUPPORTS USB

Vous trouvez ou on vous offre une clé USB (ou tout autre support à connecter). Partez du principe qu'elle est piégée et que même les plus grands spécialistes pourraient avoir du mal à s'en apercevoir. Ne la branchez jamais sur vos moyens informatiques personnels et encore moins sur vos moyens informatiques professionnels au risque de les compromettre en ouvrant un accès à un cybercriminel. Utilisez une clé USB pour vos usages personnels et une autre pour vos usages professionnels afin d'éviter que la compromission de l'une ne puisse infecter l'autre.

10 ÉVITEZ LES RÉSEAUX WI-FI PUBLICS OU INCONNUS

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et ainsi récupérer au passage vos comptes d'accès et vos mots de passe personnels ou professionnels, vos messages, vos documents ou même vos données de carte bancaire... afin d'en faire un usage délictueux. Depuis un réseau Wi-Fi public ou inconnu, n'échangez jamais d'informations confidentielles.

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :



RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr



Licence Ouverte v2.0 (ETALAB)

Document 10

[Accueil](#) > [Sécurité des systèmes d'information](#)

La sécurité numérique

La sécurité numérique est en enjeu stratégique au cœur de la transformation numérique du ministère et du service public de la Justice. La politique ministérielle de sécurité numérique garantit la protection des données et la continuité des activités, y compris en cas de cyberattaque.

Intranet du ministère de la Justice - Novembre 2022

La sécurité numérique consiste à protéger les systèmes d'informations, les informations et les moyens d'y accéder contre les actes de malveillance. Très longtemps appréhendée comme un domaine technique lié à l'informatique (cybersécurité), la sécurité numérique est maintenant un enjeu stratégique, une condition fondamentale pour mener la transformation numérique et les missions de service public de la Justice.

Afin de garantir la continuité d'activité et de préserver les données sensibles, le ministère déploie un dispositif d'ensemble qui se traduit en trois axes :

- Organisation de la gouvernance de la sécurité numérique,
- Maîtrise du risque numérique,
- Gestion des incidents de sécurité et des crises cyber.

Quels sont les types d'incident de sécurité ?

La qualification d'un événement de sécurité définit un incident de sécurité.

Un incident de cybersécurité survient suite à une cyberattaque. Les désordres peuvent varier en fonction des effets recherchés par l'attaquant pour atteindre son objectif.

Les cyberattaquants ont des profils et des motivations différents. Des groupes de hackers, des cyberterroristes, des États pratiquent de l'espionnage, du sabotage ou sont simplement motivés par l'appât du gain. Différents modes opératoires ont été répertoriés :

- **attaque en « déni de service (DDoS) »** : l'attaquant cherche à rendre indisponibles, inaccessibles, les sites Web, l'Internet, une application ou un télé-service... L'objectif est d'attirer l'attention dans l'espace médiatique pour porter des revendications politiques, militantes, idéologiques...
- **attaque sur la chaîne d'approvisionnement (supply chain)** : il peut être plus aisé pour des attaquants de passer par des partenaires ou des prestataires travaillant avec le ministère pour atteindre notre réseau. L'objectif est le contrôle du système d'information en vue de le corrompre ou de le détruire. Ce type d'attaque est le fait de groupes étatiques et paraétatique dans le cadre d'opérations d'espionnage ou de déstabilisation
- **hameçonnage (phishing)** : c'est une pratique très courante. Depuis un mail, l'attaquant souhaite que sa victime clique sur un lien qui permet d'installer un programme malveillant qui peut-être un cheval de Troie ou un rançongiciel
- **rançongiciel (ransomware)** : avec cet outil, l'attaquant va chiffrer des données et demandera une rançon en échange de la clé de déchiffrement. Actuellement, les rançongiciels volent aussi les données préalablement à leur mise hors d'état. Ce vol participe au chantage.

Comment s'organise la cybersécurité au ministère ?

L'organisation de la sécurité numérique est précisée par la [politique ministérielle de sécurité numérique](#) (PMSN) qui décline [l'instruction générale interministérielle 1337](#) du 26 octobre 2022.

Elle s'articule autour de trois chaînes complémentaires :

- **la chaîne décisionnelle** qui définit et pilote la stratégie ministérielle de sécurité du numérique. Cette chaîne repose sur des instances de gouvernance représentées par le ministre et les directeurs d'administration centrale.
- **la chaîne fonctionnelle dédiée** en charge du pilotage et du contrôle de la mise en œuvre opérationnelle de la stratégie de sécurité numérique. Cette chaîne

repose sur des instances de pilotage qui permettent de concilier les instances décisionnelles et les instances opérationnelles. Elle est représentée par le fonctionnaire de la SSI (FSSI), les conseillers à la sécurité numérique (CSN), et les responsables centraux de la SSI (RCSSI).

- **la chaîne opérationnelle dédiée** qui permet de décliner de manière concrète et pragmatique la stratégie ministérielle de sécurité numérique. Cette chaîne repose sur des **instances de suivi** représentées par le responsable du CSIRT (équipe en charge du pilotage d'incidents), le responsable du SOC (équipe en charge de la détection et du traitement des incidents), les RSSI.

Contacts

Pour l'aspect technique : prévenez votre RSSI de DIT.

Par défaut, vous pouvez contacter le centre de support national au 01.70.22.88.36.

SG/HFDS



LETTRE CYBER Avrīl – Maī 2024

Dans cette édition, nous vous proposons de vous familiariser avec les menaces de phishing et d'ingénierie sociale.

N'hésitez pas à diffuser cette lettre au sein du ministère !

Nous vous souhaitons une bonne lecture !

**Ça pourrait arriver au
ministère !**



Ce mois-ci, nous vous proposons d'imaginer ce qui pourrait arriver au ministère.

A l'approche des JOP, les acteurs malveillants deviennent de plus en plus actifs. Occasion alléchante, tous les attaquants y trouvent leur compte : « des groupes criminels en quête d'opérations crapuleuses, des hacktivistes aux ambitions plus ou moins idéologiques jusqu'aux acteurs étatiques soucieux de saper l'événement, la menace est protéiforme » (AFP, *Les JO, cible majeure de cyberattaques Protéiformes*, 15/04/2024). Ainsi, **il est important d'être vigilant tout au long de la période olympique.**

Imaginez : Un mois avant la cérémonie d'ouverture un acteur malveillant envoie des mails de phishing à un ensemble d'adresses mail d'agents du ministère. Un matin, un agent faisant le tri de sa boîte mail pleine, ouvre sans trop d'attention ce mail avec pour objet « *Travaux sur le RER E : prévoyez vos déplacements* » ou « *Achetez des places de dernière minute à moitié prix pour la cérémonie d'ouverture des JOP* ». Ne s'apercevant pas des caractéristiques du phishing, il clique sur le lien présent dans le corps du mail en apparence inoffensif mais porteur d'un virus. Ce virus s'installe et s'active au moment des JOP et paralyse le réseau du ministère, provoquant des dommages suffisamment importants pour empêcher toute activité de la juridiction, des établissements, de la plateforme interrégionale et du ministère et nécessitant l'ouverture d'une cellule de crise. L'incident est grave et le ministère va travailler en mode dégradé pendant plusieurs jours, voire des mois...

Cet exemple montre comment « un simple clic » peut provoquer des effets très graves.

La vigilance et la sensibilisation de tous les agents est donc essentielle : tous connectés, tous impliqués !



Le zoom du mois



L'ingénierie sociale, ou comment anticiper votre comportement

Certain(e)s d'entre vous ont peut-être eu l'occasion de feuilleter le *Petit traité de manipulation à l'usage des honnêtes gens*¹. Ce livre à succès met en scène et décrypte des mécanismes de manipulation simples utilisés pour obtenir des informations ou concessions impossibles à obtenir en temps normal. C'est sur ce principe que se basent les attaques d'ingénierie sociale.

L'ingénierie sociale est un type de cyberattaque qui utilise ces techniques de manipulation pour pousser la victime à agir d'une certaine manière. Elle la pousse à **se mettre en danger** (et potentiellement son organisation) ou à **divulguer des informations personnelles**.

Concrètement, ça donne quoi ?

En cybersécurité, l'utilisation de l'ingénierie sociale se fait principalement **via le phishing** (hameçonnage) sur les boîtes mail. Sans être particulièrement complexes, ces attaques exploitent nos réflexes, nos envies et nos craintes. Leur simplicité participe à leur efficacité, car elles s'appuient sur **nos réactions naturelles et notre inattention**.

La technique la plus souvent exploitée en ingénierie sociale est celle de **créer un sentiment d'urgence ou d'angoisse**. En insérant une date butoir, en accentuant le caractère anxiogène du mail, il est plus susceptible de **susciter un sentiment de stress et de pousser à l'action**. L'usurpation d'identité d'agents des forces de l'ordre pour accuser la cible d'un délit et exiger le paiement rapide

d'une amende ou le chantage à la webcam en sont des exemples connus.

À chaque cible sa méthode...

Pour réussir, l'ingénierie sociale se base aussi sur l'adaptation de l'attaque à la cible. En faisant des recherches préalables (via les réseaux sociaux notamment), un attaquant sera plus efficace dans sa tentative. On parle alors de **phishing ciblé** ou « **spear phishing** ».

Il est aussi possible de se baser sur des informations obtenues lors de recherches préalables pour **gagner votre confiance**. Face à un mail qui comporte de nombreux éléments « rassurants », on relâche plus facilement son attention. L'exemple de l'attaquant Emotet illustre bien ce cas de figure : ce dernier reprenait un fil de discussion légitime pour insérer un contenu malveillant dans la conversation.

Qui est réellement au bout du fil ?

L'ingénierie sociale implique parfois **des interactions directes**. Grâce à des informations obtenues, l'attaquant peut mener une **conversation téléphonique crédible** pour parvenir à ses fins. Par exemple, en se faisant passer pour un utilisateur légitime qui contacte l'assistance technique pour réinitialiser ses identifiants... C'est ce qui est arrivé récemment à France Travail. En passant par la hotline, les pirates ont usurpé l'identité d'employés et ont demandé la réinitialisation de leur mot de passe. Ils ont ainsi infiltré la base de données de l'organisme.

¹ R-V. Joule & J-L. Beauvois, Presses Universitaires de Grenoble, 1987.

Ce mode opératoire est également utilisé pour **usurper l'identité des hauts responsables** et ordonner une transaction financière à effectuer urgemment. En jouant sur l'**hésitation à refuser une demande faite par un supérieur**, l'attaquant peut récupérer des sommes importantes. C'est le « **whaling** » (pêche à la baleine en anglais) ou « **fraude au président** ».

Pour finir, si vous avez un doute sur un mail, vérifiez l'identité de l'expéditeur et **ne vous fiez pas uniquement au nom de l'émetteur**. **Survolez le lien URL avec la souris** pour vérifier qu'il s'agit bien d'un site de confiance. Ne téléchargez aucune pièce jointe **si vous avez le moindre soupçon**. Rappelez-vous que tout fichier fini **n'est pas envoyé en format modifiable mais en PDF** (comme les devis, les factures, etc.)

Culture d'hommes et femmes du monde

La réserve cyber

Coopération économique, coopération politique, coopération juridique ... l'Union européenne s'attèle à bien des sujets ! Quid du cyber ?

Le 6 mars dernier, l'UE a annoncé l'élaboration d'un « Cyber Solidarity Act » qui prévoit la création d'un système d'alerte sur l'ensemble du territoire de l'UE dans le but de détecter et signaler des potentielles attaques d'origine cyber visant un ou plusieurs pays. En parallèle, le « Cyber Solidarity Act » prévoit un système d'urgence incluant une assistance mutuelle qui sera dispensée par une « réserve cyber ». Constituée de plusieurs milliers d'intervenants, sur la base du volontariat, elle servira de support à l'effort de défense en cas d'attaque.

Par ailleurs, dans la perspective des JOP, le ministère de la Justice vient également de créer un vivier cyber pour renforcer le dispositif de gestion des incidents de sécurité numérique et les capacités d'intervention en services déconcentrés.

Les agents du vivier cyber sont recrutés sur la base du volontariat et mobilisés en cas d'incident majeur par la cellule de crise ministérielle. Dans ce cadre les agents sont déchargés temporairement de leur service, après accord de leur hiérarchie, pour intervenir en renfort d'un DIT.

A ce jour, presque 100 agents des différentes directions du ministère se sont portés volontaires. Ils bénéficieront au cours de l'année de formations spécifiques.

En cas de doute, contactez le numéro unique d'alerte cybersécurité, joignable 24h/24 au :

01 70 22 88 36

Ou adressez votre message à

support.csn@justice.gouv.fr

3

Document 12

Les risques liés au numérique tendent à se diversifier

GPOMAG.fr [Anne Del Pozo](#) 13 mars 2022 Dernière mise à jour : 16 octobre 2024

Depuis l'explosion du digital, et en particulier de l'Internet, les entreprises sont confrontées à de nombreux risques liés au numérique qui ne se limitent pas à la criminalité. Les menaces sont aujourd'hui nombreuses et protéiformes, et les attaques sont menées à des fins économiques et financières, de déstabilisation, d'espionnage ou encore de sabotage.

Ce contexte de risques qui était déjà très important en 2020 et 2021, notamment au regard du développement du télétravail, devrait persister en 2022, voire se renforcer et ce, dans toutes les entreprises quelles que soient leur taille et leur secteur d'activité.

Toutes **les entreprises qui utilisent le numérique** sont potentiellement **exposées à différents risques**. La liste de ces risques ne saurait en revanche être exhaustive, tellement il en existe. Certains concernent plus spécifiquement un secteur d'activité.

Par exemple, une entreprise de logistique pourrait avoir une faille dans son système de gestion et prendre un important retard, une société de services pourrait décaler tous ses rendez-vous avec un logiciel de planning piraté, un livreur pourrait mélanger toutes ses adresses avec un logiciel défaillant... Il existe ainsi autant de risques que d'entreprises qui utilisent des logiciels.

Néanmoins, certains d'entre eux concernent toutes les entreprises. C'est notamment le cas des cyber risques dont la dynamique s'est encore renforcée en 2021.

Selon le **baromètre 2021 du Césin** (Le club des experts de la sécurité de l'information et du numérique) sur la cybersécurité des entreprises françaises, plus d'une entreprise sur deux (54 %) en France déclare ainsi avoir subi entre une et trois attaques cyber au cours de l'année 2021. Un chiffre qui tient uniquement compte des attaques réussies ayant eu des répercussions flagrantes pour les victimes.

Il convient par ailleurs de souligner que l'ampleur et la virulence des attaques ne cessent d'augmenter. En effet, 6 entreprises sur 10 ont connu des conséquences sur leur business suite à une telle attaque, avec pour principaux impacts une perturbation de la production (21 %) et/ou une compromission d'information (14 %) et/ou une indisponibilité du site Web pendant une période significative.

Le « phishing », principal vecteur de cyberattaque

Le baromètre du Césin souligne également que le « **phishing** » (ou hameçonnage) reste, pour 73 % des responsables de la sécurité des systèmes d'information (RSSI) interrogés le principal **vecteur pour dérober des identifiants** et démarrer une **infiltration** ou une **attaque multi-phases**.

« Ce type d'attaque vise à obtenir du destinataire d'un email ou d'un lien d'apparence légitime pour qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services externes afin de dérober de l'argent, des accès d'un plus haut niveau ou des informations sensibles, explique Julien Gonzalès, président de Z-Index. Le Phishing peut également être utilisé dans des attaques plus ciblées pour essayer d'obtenir d'un employé ses identifiants d'accès aux réseaux professionnels auxquels il peut avoir accès. Cette attaque repose généralement sur une usurpation d'identité de l'expéditeur (personne morale ou physique) afin de duper le destinataire qu'il invite à ouvrir une pièce jointe malveillante ou à suivre un lien vers un site Web malveillant ».

Une fois cette première machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du système d'information de l'organisation constituant la véritable cible. Dès lors que sa première victime est compromise, l'attaquant cherchera à obtenir des droits d'administrateur pour pouvoir rebondir et s'implanter sur les postes de travail et serveurs de l'organisation où sont stockées les informations convoitées.

Easyjet en a ainsi fait les frais en mai 2020 puisque 9 millions de données ont été piratées. Il s'agissait alors principalement de données clients comme des adresses email ou des itinéraires de voyage. Cependant, plus de 2 000 informations bancaires ont été illégalement consultées. Ces faits laissent présager d'un risque important de Phishing, bien que l'entreprise ait rapidement prévenu les clients concernés. La rapidité de prise en charge de cette cyberattaque n'a par ailleurs pas empêché une perte de confiance de millions d'utilisateurs et une plainte collective montée par plus de 10 000 clients, ce qui pourrait coûter plusieurs millions de livres à la compagnie aérienne britannique.

Le « ransomware » fait de plus en plus de victimes

Le « **ransomware** » (ou rançongiciel) est également une **technique courante de la cybercriminalité**. Elle consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

Une attaque dont a, par exemple, été victime Bouygues Construction en 2020. À la suite de l'intrusion d'un Ransomware dans son système d'information bloquant l'accès aux données internes, l'entreprise a vu ses fonctions support paralysées. La réactivité du groupe avec la suspension automatique du système informatique n'aura pas pu éviter la main mise par les pirates sur des données confidentielles. Ces dernières seraient rendues moyennant une rançon de plusieurs millions de dollars... À noter que les activités opérationnelles du groupe n'ont pas été paralysées.

Selon le Césin, les attaques par Ransomware ont ainsi touché une entreprise sur cinq en 2021. Une tendance qui pourrait progresser en 2022.

C'est tout du moins ce qui ressort du dernier baromètre d'Anozr Way, Start-up spécialisée dans la lutte contre le piratage et l'analyse cyber. L'observation des mécanismes à l'œuvre en 2021 a démontré que les données récupérées lors des attaques sont massivement utilisées par les groupes de « hackers », **explique Anozr Way**.

Et cela n'augure vraiment rien de bon pour 2022 : pour une seule entreprise attaquée en France, ce sont en moyenne 150 autres qui sont en danger. La Startup estime par ailleurs que les pertes attribuées à ces cyberattaques correspondent à 2,5 milliards d'euros de chiffre d'affaires cumulé pour les sociétés victimes. Entre les mois de juillet et novembre 2021, Anozr Way évalue ainsi à 200 % la hausse du nombre des organisations ciblées par des rançongiciels au niveau mondial.

Le nombre d'attaques DDoS progressent

Exploitation des vulnérabilités, arnaques au président, tentatives de connexions frauduleuses, acquisitions de noms de domaines illégitimes ou encore les **attaques DDoS** (déni de service) sont également des **cyberattaques courantes**, voire en forte progression pour les attaques DDoS.

Ces dernières ont augmenté de 29 % sur l'année 2021 et de 175 % pour le seul quatrième trimestre (rapport DDoS Attack Trends for Q4 2021).

« Les attaques DDoS visent à rendre un serveur, un service ou une infrastructure indisponibles, **précise Julien**

Gonzalès. Elles peuvent prendre différentes formes : une saturation de la bande passante du serveur pour le rendre injoignable ou un épuisement des ressources système de la machine, l'empêchant ainsi de répondre au trafic légitime ».

Alors en pleine bataille contre la première vague de la Covid-19, l'Assistance Publique-Hôpitaux de Paris a ainsi été la cible d'une telle attaque qui a rendu une partie des serveurs de l'AP-HP inaccessibles, à cause d'une surcharge de requêtes inutiles. Une heure durant, l'AP-HP a dû couper les accès aux outils internes et aux emails pour les salariés alors en télétravail.

Les attaques indirectes par rebond via un prestataire entrent dans le top 10

Les « **attaques indirectes par rebond via un prestataire** », qui augmentent de 5 % pour atteindre les 21 %, entrent pour leur part dans le Top 10 des cyberattaques ! Une progression qui reflète la réalité d'une année 2021 marquée par les attaques sur la Supply Chain logicielle avec les incidents SolarWinds et Log4J.

Cela fait plusieurs années d'ailleurs que l'**Anssi** (Agence nationale de la sécurité des systèmes d'Information) **s'inquiète des faiblesses de la Supply Chain** des grandes entreprises, qui repose souvent sur des TPE et PME moins formées aux défis cyber. Si elles ont souvent cherché à se protéger des faiblesses de leurs prestataires, elles n'ont pas toujours mesuré l'importance des acteurs de leur Supply Chain logicielle.

La perte de données, principal risque lié au numérique

Au-delà de la cybercriminalité, la **perte de données** représente également pour les entreprises un **risque important lié au numérique**. Dès lors qu'une entreprise ne sauvegarde pas ses données sur deux sites distants, elle peut se trouver confrontée à des difficultés d'accès à ses données, voire tout perdre du jour au lendemain.

C'est notamment ce qui s'est passé pour un certain nombre de sociétés lors de l'incendie d'un datacenter d'OVHcloud en mars 2021, qui regroupait 14 000 serveurs. Suite à cet incendie, 120 000 services se sont retrouvés partiellement ou totalement à l'arrêt, parmi lesquels le site data.gouv.fr qui est resté inaccessible quelques heures, mais également les sites des démarches simplifiées de l'État, de l'aéroport de Strasbourg, du parti de François Asselineau ou encore du club de rugby de Clermont-Ferrand, etc.

D'autre part, un certain nombre de clients ayant conclu un contrat d'hébergement simple, sans service de sauvegarde associé, ont perdu, temporairement ou définitivement leurs données dans cet incendie. Plusieurs clients d'OVHcloud, qui ont vu leurs données partir en fumée dans l'incendie des datacenters du groupe à Strasbourg le 10 mars dernier, se sont d'ailleurs regroupés pour lancer une action en justice commune impulsée et représentée par le cabinet d'avocats Ziegler & Associés, spécialisé dans ce type de contentieux. Selon le cabinet d'avocats, les préjudices subis par ces entreprises s'échelonnent entre 10 000 euros et 1,9 million d'euros.

La e-réputation peut ternir l'image de l'entreprise

Le **numérique** peut également exposer l'entreprise à des **risques réputationnels**. Un risque qui peut toucher tout type d'entreprises, mais aussi des travailleurs indépendants, artisans, commerçants, dès lors qu'ils ont un site en ligne. Si les avis ou retours clients sont mauvais, il sera alors difficile de s'en défaire, et la **réputation de l'entreprise** en sera ternie. D'où la nécessité de surveiller sa e-réputation.

Manquement au RGPD : attention à la facture !

« Un autre risque lié au numérique concerne la responsabilité et les obligations des entreprises en matière de protection des données clients, **explique Richard Lamy, directeur du Programme de confiance de Docaposte**.

Et c'est le cœur du métier d'un prestataire de service de confiance. À noter que le **manquement au Règlement général sur la protection des données (RGPD) expose en effet l'entreprise à des sanctions**, allant du simple rappel à l'ordre à une injonction de se mettre en conformité pouvant être assortie d'une astreinte jusqu'à 100 000 euros par jour de retard, en passant par le retrait d'une certification, ou une amende administrative pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial.

Toutes les entreprises établies sur le territoire de l'Union européenne et qui stockent des données personnelles sont concernées (le stockage de données est une forme de traitement) par la RGPD. Dans le cadre de cette réglementation, le responsable d'un fichier client ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime ; les informations enregistrées doivent être pertinentes et strictement nécessaires au

regard de la finalité du fichier ; il n'est pas possible de conserver des informations sur des personnes physiques dans un

Les chiffres de la cybersécurité

- **Plus d'une entreprise sur deux** (54 %) en France déclare avoir subi entre une et trois attaques cyber au cours de l'année 2021 (Baromètre 2021 du Césin sur la cybersécurité des entreprises françaises).
- **Plus de 80 % des événements de cybersécurité** impliquent des attaques de phishing (Threat Report 2020, Teiss) ; Google a découvert plus de 2.1 millions de sites de phishing en janvier 2021.
- **2 entreprises françaises sur 3 ont subi au moins une tentative de fraude cette année**, et 1 entreprise sur 5 a subi plus de 5 attaques. Un cadre qui peut en effet paraître plus propice à la fraude et à la cybercriminalité, surtout dans un contexte qui a poussé les entreprises à une adaptation très rapide et donc potentiellement moins contrôlée (Euler Hermes/DFCG, 2021).

fichier pour une durée indéfinie.

Une **durée de conservation** précise doit être **fixée**, en fonction du type d'information enregistrée et de la finalité du fichier ; le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations ; enfin, il faut respecter le droit des personnes.

À titre d'exemple, en 2020, l'entreprise H&M a été condamnée à 35 millions d'euros pour surveillance illégale de ses propres employés. H&M avait notamment créé des profils de ses employés qui contenaient des informations médicales (symptômes à chaque absence pour maladie, détails de la maladie en question, détails des diagnostics, etc.), ainsi que des informations relatives aux croyances religieuses, des détails précis relatifs à leur vie privée autant qu'à leurs problèmes personnels.

Or, une telle collecte de données personnelles est interdite par le RGPD, et viole le principe de minimisation.

Toutes les entreprises sont concernées par les risques liés au numérique

Les **risques liés au numérique** représentent ainsi une **menace omniprésente** et « **invisible** » qui n'épargne ni les particuliers, ni les entreprises ou les organisations. Ainsi, d'après l'ANSSI, 11 % des cyberattaques ont, en 2021, concerné des hôpitaux et 20 % des collectivités territoriales, le reste visant des entreprises.

Les **petites et moyennes entreprises** s'avèrent être d'ailleurs – sans surprise – des **cibles privilégiées**, représentant 44 % des organisations touchées par des ransomwares. Plus vulnérables et moins résilientes, ces petites et moyennes entreprises restent encore en 2021 moins bien protégées et moins alertées des répercussions d'une attaque.

En moyenne, une entité perd 27 % de son chiffre d'affaires annuel dans une attaque (Anozr Way). Pour une petite entreprise, cela peut même l'obliger à mettre la clé sous la porte. En termes de secteurs ciblés, les sociétés de la finance et de l'assurance arrivent en tête, suivies de celles opérant dans les services tertiaires, le commerce et l'industrie.

Les Français ont également du souci à se faire concernant la **fuite de leurs données personnelles**. À partir d'un seul échantillon analysé par Anozr Way, 680 000 français ont été directement concernés en 2021 par l'exposition de leurs données personnelles, du fait des vols de données des entreprises piratées par ransomware.

En effet, chaque entité victime de rançongiciel expose en moyenne 5 500 personnes (collaborateurs, clients, patients). Ces données concernent des documents d'identité (carte d'identité, passeport, numéro de sécurité sociale), mais aussi des informations médicales et des données financières (RIB, prêts). Ainsi, les risques liés au numérique sont vraiment très divers et ne cessent de se développer. Les hackers quels qu'ils soient restent d'ailleurs très inventifs et les attaquent continuent de se diversifier, ce qui complexifie d'autant la tâche des entreprises en termes de protection de leur système d'information et de leurs données.

Sans compter qu'elles doivent aussi **veiller à la réglementation en matière de protection des données**, et ce dans un environnement de plus en plus digital et où le développement des nouvelles technologies ouvre sans cesse de nouvelles brèches...

¹ Le principe de minimisation prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

Document 13

Cybersécurité : le défi de la formation des dirigeants publics

Publié dans La Gazette des Communes le 06/12/2023 • Par Auteur associé • dans : Opinions, Toute l'actu RH



Une nouvelle étude, récemment publiée, expose, à nouveau, un niveau de prise en compte du risque cyber par les dirigeants des collectivités territoriales qui reste globalement insuffisant. Elle pointe un niveau de vulnérabilité qu'il convient de prendre au sérieux.

Marc Bidan, Olivier Lasmoles, et Rémy Février respectivement Auteurs historiques The Conversation France, SKEMA Business School et, Conservatoire national des arts et métiers (CNAM)

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.

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 les 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 réhabilitaires – 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 »

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 « 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, managers, 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".