

NUMÉRIQUE · SÉCURITÉ DE L'ÉTAT

Personne n'est à l'abri ! L'ANSSI et la DINUM, chargées de protéger les données de l'État, victimes à leur tour d'une fuite de données

Les deux services du Premier ministre qui ont pour mission de sécuriser le numérique de l'État figurent eux-mêmes dans la liste des victimes. Le point de situation publié par l'ANSSI le 30 septembre 2026 recense 99 violations de données signalées en deux mois dans les ministères. Le constat le plus préoccupant n'est pas l'ampleur des fuites, mais la banalité des failles qui les ont rendues possibles. Décryptage technique, chronologie et propositions.

Par Philippe Agnelli, ingénieur informatique · Élysée Conseils — Projet 2027 · 1^{er} octobre 2026 · Lecture : 15 min

L'ESSENTIEL

- Le laboratoire d'innovation de l'ANSSI a vu **118 comptes** compromis, et la **DINUM** deux de ses instances Metabase, via une faille notée **10 sur 10** pour laquelle un correctif existait depuis le 6 août 2026.
- Depuis le 1^{er} août 2026, **99 violations de données** ont été signalées à l'ANSSI dans les services de l'État, dont **67 confirmées**.
- Enseignants, élèves, contribuables, propriétaires : plusieurs dizaines de millions de Français sont potentiellement concernés, dont **48 millions de propriétaires** pour la seule plateforme Zéro Logement Vacant.
- À la DGFIP, l'attaquant a exfiltré **11 Go** de données en une nuit sans qu'aucune alerte ne se déclenche ; la réinitialisation du mot de passe n'a même pas coupé sa session.

- Le principe qui aurait fermé la plupart de ces portes, un second facteur indépendant reçu sur un autre appareil, je l'avais breveté en France dès l'an 2000.
- Le Projet 2027 propose six mesures, dont l'accès aux données sensibles par la carte d'identité, validé par un registre central des habilitations tenu par l'ANSSI.

SOMMAIRE

1. [Que s'est-il passé à l'ANSSI et à la DINUM ?](#)
2. [Quelle est l'ampleur des fuites de données de l'État ?](#)
3. [Comment une seule faille a-t-elle ouvert neuf ministères ?](#)
4. [Anatomie d'une intrusion : que révèle le rapport sur la DGFIP ?](#)
5. [Que fait l'État pour reprendre la main ?](#)
6. [Mon regard d'ingénieur : une solution connue depuis vingt-cinq ans](#)
7. [Ce que propose le Projet 2027](#)
8. [Que peut faire chaque citoyen ?](#)

01

Que s'est-il passé à l'ANSSI et à la DINUM ?

Les deux gardiens du numérique de l'État ont été touchés par la même faille, exploitée dans des outils de tableaux de bord qui n'avaient pas été mis à jour à temps.

L'Agence nationale de la sécurité des systèmes d'information (ANSSI)¹ est l'autorité chargée de défendre les systèmes de l'État contre les cyberattaques. La direction interministérielle du numérique (DINUM)² pilote la transformation numérique des administrations et opère plusieurs services communs, dont ProConnect, l'identifiant unique des agents publics. Toutes

deux sont rattachées au Premier ministre. Toutes deux figurent dans le point de situation que l'ANSSI a publié le 30 septembre 2026 sur les violations de données touchant l'État.

Au laboratoire d'innovation de l'ANSSI, l'exploitation d'une vulnérabilité du logiciel Metabase, un outil libre de visualisation de données, a conduit à la compromission de **118 comptes utilisateurs**, dont une trentaine de comptes externes. Les attaquants ont emporté des identifiants, des adresses électroniques, des mots de passe hachés et des statistiques d'utilisation. L'Agence a mis à jour ses instances, renouvelé l'ensemble des mots de passe et désactivé les comptes inutilisés depuis plus de trois mois.

À la DINUM, deux instances Metabase ont été compromises : celle de ProConnect et celle de Nuage-Public. Les données exfiltrées concernent des informations administratives d'organismes publics (SIREN, SIRET, budgets, effectifs), des métadonnées de contributions à des logiciels libres et des historiques de connexion anonymisés. La DINUM précise que ces données étaient déjà publiques. Elle a corrigé les failles, réinitialisé ses secrets techniques et supprimé les comptes que l'attaquant avait créés.

Un détail technique mérite l'attention : des mots de passe « hachés » ne sont pas des mots de passe en clair, mais leur empreinte mathématique. Ils restent exploitables hors ligne par des attaques par dictionnaire, d'autant plus vite que les mots de passe d'origine sont courts ou réutilisés ailleurs. C'est pourquoi l'ANSSI a fait renouveler l'ensemble des mots de passe, et non les seuls comptes dont l'usage frauduleux était avéré.

CE QU'ON POURRAIT CROIRE

Ces fuites restent sans gravité, puisque les données de la DINUM étaient publiques et que les mots de passe de l'ANSSI étaient hachés.

CE QU'IL FAUT RETENIR

Le préjudice est limité, mais le signal est fort : si les services chargés d'imposer les règles de sécurité n'ont pas appliqué un correctif disponible, aucune administration ne peut se croire protégée par défaut.

Quelle est l'ampleur des fuites de données de l'État ?

En deux mois, 99 violations de données ont été signalées à l'ANSSI dans sept grands pôles ministériels, et plusieurs dizaines de millions de Français sont potentiellement exposés.

99

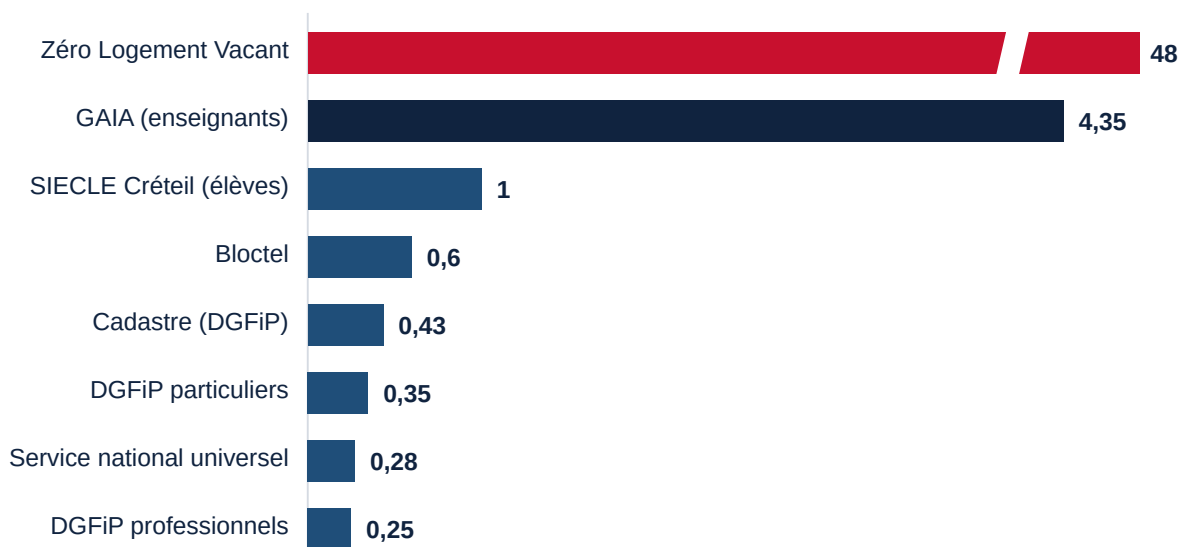
violations de données portées à la connaissance de l'ANSSI entre le 1^{er} août et la fin septembre 2026 ; 67 sont confirmées, dont 32 encore traitées directement par l'Agence.

Source : ANSSI, REACTIV — Point de situation, septembre 2026. Bilan provisoire, appelé à évoluer.

Le rapport passe en revue l'Éducation nationale, les Affaires étrangères, Bercy, la Transition écologique, le Travail, l'Agriculture et les services du Premier ministre. Aucun grand pôle de l'État n'est épargné. L'Éducation nationale signale à elle seule des incidents dans plus d'une dizaine d'académies depuis juillet.

PRINCIPALES VIOLATIONS DE DONNÉES RECENSÉES PAR L'ANSSI (ÉTÉ 2026)

SERVICE TOUCHÉ	PERSONNES OU ÉLÉMENTS EXPOSÉS	PORTE D'ENTRÉE
Zéro Logement Vacant (Transition écologique)	48 millions	Propriétaires de logements ; instance Metabase compromise selon les premiers éléments
GAIA (Éducation nationale)	4,35 millions	Enseignants : identité, affectation, grade, indemnités ; intrusion avec latéralisation
SIECLE, académie de Créteil	1 million	Élèves, responsables légaux et enseignants
Bloctel (Bercy)	600 000	Compte professionnel d'une entreprise : numéros identifiés par différence entre deux listes
Serveur cadastral (DGFIP)	434 000	Poste infecté d'un géomètre-expert, second facteur par courriel contourné
DGFIP, particuliers	353 000	Identifiants d'agents volés par <i>infostealer</i> , portail sans double authentification
Service national universel	275 000	Faible IDOR : accès à des fiches sans contrôle d'identité
DGFIP, professionnels	252 000	Même chaîne d'attaque que pour les particuliers
Qualicharge (bornes de recharge)	102 000	Sessions de recharge et une centaine de comptes techniques ; Metabase
France VAE (Travail)	Totalité	Ensemble des données des utilisateurs ; Metabase, compromis le 8 août
Laboratoire d'innovation de l'ANSSI	118 comptes	Metabase : identifiants, courriels, mots de passe hachés
DINUM (ProConnect, Nuage-Public)	2 instances	Metabase : données administratives déjà publiques



La barre Zéro Logement Vacant est tronquée : à l'échelle, elle mesurerait plus de dix fois la barre GA

Source : ANSSI, REACTIV — Point de situation, septembre 2026. Les effectifs peuvent se recouper d'un incident à l'autre.

Derrière ces chiffres, il y a des données qui ne se remplacent pas. Un mot de passe se change en une minute ; une date de naissance, une adresse, un revenu fiscal ou la composition d'un foyer, non. Une fois sur le marché noir, ces informations alimentent pendant des années les escroqueries par téléphone, par courriel ou par SMS, d'autant plus crédibles qu'elles s'appuient sur des données exactes.

03

Comment une seule faille a-t-elle ouvert neuf ministères ?

Par une injection SQL dans la page de réinitialisation du mot de passe de Metabase : une requête anonyme suffisait à devenir administrateur de l'outil.

Metabase est un logiciel de tableaux de bord : on le branche sur des bases de données pour produire des graphiques et des statistiques. C'est précisément ce qui en fait une cible de choix. Celui qui prend le contrôle de l'outil voit tout ce que l'outil voit.

La faille, référencée CVE-2026-72898, se loge dans la fonction de réinitialisation du mot de passe. Cette page est, par construction, accessible sans être connecté. En y glissant des instructions SQL, le langage qui sert à interroger les bases de données, un attaquant anonyme fait exécuter ses propres commandes dans la base interne de Metabase et s'octroie les droits d'administrateur de l'instance. L'éditeur, comme l'agence fédérale américaine de cybersécurité, lui attribue la note de gravité maximale, 10 sur 10 sur l'échelle CVSS.

LA CHAÎNE D'ATTAQUE METABASE, EN QUATRE ÉTAPES



Aucun mot de passe, aucune interaction d'un utilisateur : c'est ce qui vaut à la faille la note maximale de 10 sur 10.

Sources : CERT-FR, alerte CERTFR-2026-ALE-010 ; ANSSI, REACTIV — Point de situation, septembre 2026.

Une course contre la montre perdue d'avance

Les premières attaques visent le service en ligne de l'éditeur dès le 3 août. Metabase publie son correctif le 6 août. Le 10 août, la faille reçoit son identifiant officiel et des programmes d'exploitation circulent publiquement. Le 11 août, l'agence américaine CISA l'inscrit dans son catalogue des vulnérabilités activement exploitées et donne trois jours aux administrations fédérales, jusqu'au 14 août, pour la corriger. En France, le CERT-FR publie une alerte et l'ANSSI demande à tous les ministères d'identifier leurs instances.

Pourtant, neuf instances ministérielles ont été compromises. France VAE l'a été dès le 8 août, deux jours après la publication du correctif. Ce délai illustre une réalité que je connais bien comme ingénieur : dès qu'un correctif est publié, les attaquants comparent l'ancienne et la nouvelle version du code pour comprendre la faille. La publication d'un correctif déclenche donc une course, et chaque jour sans mise à jour devient un jour d'exposition maximale.

3 jours

C'est le délai donné aux administrations fédérales américaines pour corriger la faille Metabase après son inscription au catalogue des vulnérabilités activement exploitées (11-14 août 2026).

Source : CISA, alerte du 11 août 2026 ; The Hacker News, août 2026.

IDÉE REÇUE

Le logiciel libre est en cause : Metabase est un outil open source.

RÉALITÉ

L'éditeur a publié son correctif en trois jours. Un logiciel, libre ou propriétaire, devient dangereux lorsqu'il n'est pas maintenu. La question est celle de la discipline de mise à jour et de l'exposition sur Internet d'outils internes, pas celle de la licence.

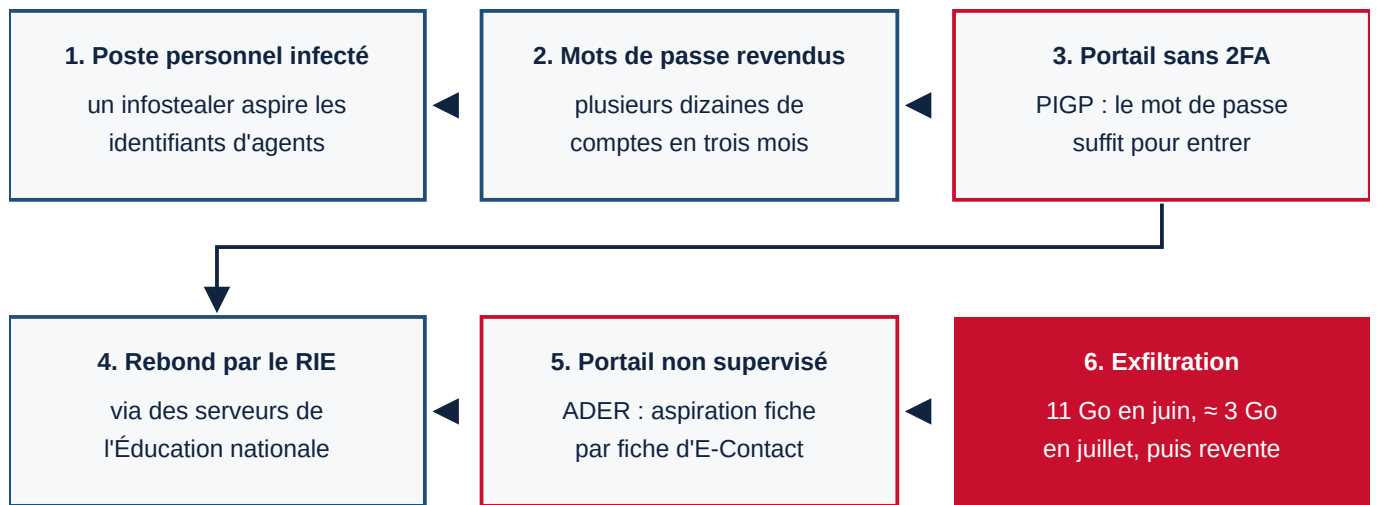
04

Anatomie d'une intrusion : que révèle le rapport sur la DGFIP ?

Trois mois d'intrusion, des dizaines de mots de passe volés, des gigaoctets exfiltrés la nuit, et une découverte par la revendication des pirates eux-mêmes.

Le rapport d'incident que l'ANSSI a consacré à la DGFIP, remis au Premier ministre le 24 septembre et rendu public le 29 septembre 2026, est un document rare : une reconstitution heure par heure d'une intrusion dans une grande administration. Son verdict tient en une phrase :

La compromission « n'est pas la conséquence d'une attaque sophistiquée ».³



RIE : réseau interministériel de l'État. PIGP et ADER : portails d'accès aux applications de la DGFIP.

Source : ANSSI, rapport d'incident n° 3033/ANSSI/SDO/NP du 23 septembre 2026.

Les identifiants volés, pas devinés

L'ANSSI n'a relevé aucune attaque par force brute ni par « bourrage d'identifiants ».

L'attaquant ne cherchait pas les mots de passe : il les avait déjà. Ils provenaient très probablement de logiciels espions installés sur des ordinateurs que la DGFIP n'administre pas, notamment des appareils personnels d'agents et des postes d'organismes partenaires. Le portail PIGP, porte d'entrée de l'attaquant, ne demandait aucun second facteur aux agents.

Le rebond par le réseau interministériel

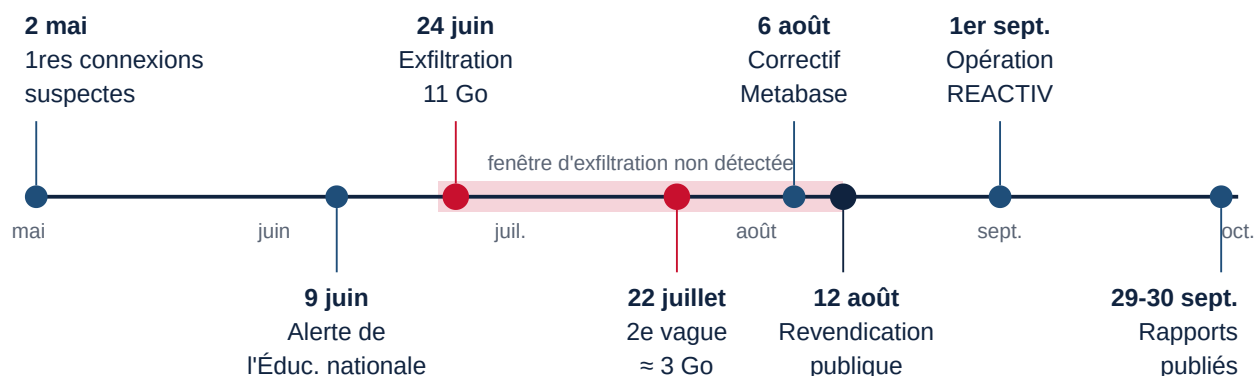
Le réseau interministériel de l'État (RIE) relie les administrations entre elles. Des serveurs de l'Éducation nationale déjà compromis ont servi de tremplin pour atteindre le portail ADER de la DGFIP. L'Éducation nationale avait pourtant partagé 17 marqueurs d'attaque avec tous les ministères dès le 9 juin. L'ANSSI juge la segmentation du réseau trop permissive : des sites sans besoin apparent d'accéder aux infrastructures de la DGFIP pouvaient s'y connecter.

Une session qui survit à la réinitialisation du mot de passe

Le 23 juin au soir, une alerte automatique se déclenche sur des recherches suspectes. Le lendemain matin à 10 h 40, le centre de supervision réinitialise le mot de passe du compte. Mais la session ouverte par l'attaquant n'est pas révoquée : l'exfiltration, commencée à 4 h 26,

se poursuit jusqu'au 25 juin à 2 h 31. Changer la serrure ne sert à rien si l'intrus est déjà dans la maison et que personne ne lui demande de sortir.

CHRONOLOGIE DE L'ÉTÉ 2026



Sources : ANSSI, rapport d'incident DGFIP et point de situation REACTIV, septembre 2026 ; avis de sécurité Metabase, 6 août 2026.

Cinq signaux qui n'ont pas sonné

L'ANSSI dresse la liste des indices qui, corrélés, auraient dû déclencher l'alarme. Aucun n'a été rapproché des autres, en partie parce que le portail ADER n'était pas placé sous la surveillance du centre de supervision de la DGFIP.

SIGNAL	CE QUI S'EST PASSÉ	PARADE STANDARD
Volume	11 Go en 3 jours	Quotas de données par compte et par période
Rythme	Aspiration automatisée, une requête par fiche	Limitation du nombre de requêtes (<i>rate limiting</i>)
Horaires	Connexions nocturnes, exfiltration lancée à 4 h 26	Alerte sur les accès hors des plages habituelles
Provenance	Adresses de VPN, adresses réputées malveillantes, géolocalisation en Inde	Filtrage par réputation et géolocalisation des adresses IP
Session	Session active malgré la réinitialisation du mot de passe	Révocation de toutes les sessions à chaque réinitialisation

L'intrusion n'a été découverte que le 12 août, lorsque l'attaquant, sous le pseudonyme Zerobytes, a revendiqué le vol sur un forum. Il annonçait 678 437 enregistrements, un chiffre supérieur au bilan officiel de 353 000 particuliers et 252 000 professionnels. L'ANSSI a prévenu la DGFIP moins de trois heures après la revendication. Mais l'exfiltration principale datait de sept semaines.

05

Que fait l'État pour reprendre la main ?

L'État a lancé l'opération REACTIV le 1^{er} septembre 2026 et accéléré sa feuille de route de sécurité numérique, après un plan de 200 millions d'euros annoncé au printemps.

Le 1^{er} septembre 2026, le Premier ministre⁴ a demandé à l'ANSSI de lancer REACTIV, pour « REponse & ACTion Interministérielle face aux Violations de données ». L'Agence a basculé ses efforts opérationnels vers les ministères. Son autorité est renforcée sur deux points : elle

peut leur faire prendre, dans des délais contraints, les mesures d'urgence nécessaires pour protéger les données des citoyens, et elle centralise la communication technique de crise.

Les premiers résultats sont réels. Grâce aux marqueurs d'attaque partagés par l'ANSSI, les Douanes ont relié la compromission de trois comptes de messagerie à celle d'un serveur d'échange avec des prestataires, aujourd'hui définitivement coupé. Au ministère de la Transition écologique, plus de 300 comptes compromis ont été détectés sur l'application Bureau numérique, qui donne accès à une messagerie partagée entre ministères ; la double authentification y est désormais activée pour tous. À la DGFIP, l'accès des agents aux portails ADER et PIGP depuis l'extérieur a été coupé et ne devrait pas être rouvert.

Ces mesures s'ajoutent au plan annoncé le 30 avril 2026 après l'attaque contre l'Agence nationale des titres sécurisés : 200 millions d'euros pris sur les crédits de France 2030, la fusion de la DINUM et de la DITP en une autorité numérique de l'État, l'affectation des amendes de la CNIL à un fonds de modernisation, et l'obligation de consacrer 5 % des budgets numériques de chaque ministère à la cybersécurité dès 2027. La feuille de route publiée le 9 avril 2026 fixe aux ministères une quarantaine d'actions, dont l'authentification multifacteur pour tous les administrateurs de systèmes d'information au 31 décembre 2026.

CE QUI EST ACQUIS

Un diagnostic public, des rapports d'incident publiés, un pouvoir d'injonction confié à l'ANSSI et des crédits débloqués.

CE QUI RESTE À CONSTRUIRE

Une culture de la mise à jour et de la double authentification dans chaque service, une supervision applicative et une responsabilité clairement identifiée pour chaque base de données.

Mon regard d'ingénieur : une solution connue depuis vingt-cinq ans

Les recommandations de l'ANSSI en 2026 rejoignent les principes de sécurisation des transactions sur réseaux ouverts que j'ai brevetés en France dès l'an 2000.

Je suis ingénieur informatique. À la fin des années 1990, j'ai travaillé sur une question qui paraissait alors futuriste : comment payer sur Internet sans jamais faire circuler d'information bancaire sur un réseau ouvert à la fraude ? Ces travaux ont donné lieu à deux dépôts de brevets en France, en 2000 et en 2001, le premier étendu à l'international⁵.

Le principe reposait sur trois niveaux de sécurité indépendants : une clé personnelle d'identification, un code de confirmation à usage unique envoyé sur un appareil personnel par un canal distinct, ouvert pour l'occasion par l'opérateur téléphonique, et une transformation secrète de ce code, connue du seul utilisateur. Mon brevet de 2000 pose qu'un attaquant peut dérober deux des trois niveaux sans que la transaction soit compromise, et que toute anomalie est enregistrée et signalée à l'utilisateur.

PRINCIPE	BREVET FR 2807247 (DÉPOSÉ EN 2000)	RECOMMANDATIONS DE L'ANSSI (2026)
Plusieurs facteurs	Clé personnelle, code reçu sur un appareil personnel, transformation secrète du code	Authentification multifacteur sur tous les applicatifs
Canal séparé	Code envoyé sur l'appareil personnel par un canal ouvert pour l'occasion	Second facteur livré sur un appareil différent de celui du premier
Résistance au vol	Deux des trois niveaux peuvent être dérobés sans compromettre la transaction	Second facteur résistant à la compromission du premier ; code par courriel jugé insuffisant
Minimisation	Aucune information bancaire ne circule sur le réseau public	Accès limité aux seules données nécessaires, plafonds de consultation
Anomalies	Toute anomalie est détectée, enregistrée et signalée	Corrélation des signaux suspects, alertes et blocage automatique

Vingt-six ans plus tard, j'en tire une leçon qui n'est pas technologique, mais organisationnelle. Les principes d'une authentification robuste sont connus, documentés et brevetés depuis un quart de siècle. Le code SMS est aujourd'hui banal sur les applications bancaires. Ce qui manque à l'État n'est pas l'invention : c'est la discipline de l'appliquer partout, tout le temps, y compris sur l'outil de statistiques installé par une petite équipe et oublié dans un coin du réseau.

07

Ce que propose le Projet 2027

Faire de l'hygiène numérique une obligation de résultat, avec un responsable identifié pour chaque base de données de l'État.

La sécurité des données publiques ne se décrète pas : elle se construit service par service. Les incidents de l'été montrent que les règles existent, que les outils existent, et que la difficulté se

situé dans leur application. Le Projet 2027 retient le principe qui guide l'ensemble de ses chapitres institutionnels : une compétence, un responsable, un euro.

Une carte, un registre, une autorisation

Je propose que l'accès aux données sensibles de l'État passe par la carte d'identité électronique. Sa puce contient une clé qui ne la quitte jamais : un logiciel espion peut voler un mot de passe, pas la carte. À chaque connexion, l'application ne décide plus seule : elle interroge automatiquement un registre central des habilitations, tenu par l'ANSSI et protégé au plus haut niveau, qui confirme ou refuse le droit d'accès.

Ce registre est chiffré, et chaque modification y est scellée par une empreinte cryptographique dans un journal infalsifiable. Quiconque s'ajouterait des droits pour pirater un système laisserait une trace signée de son nom. À terme, cette même carte a vocation à réunir nos autres titres, comme la carte Vitale ou le permis de conduire : une seule carte, pour un État plateforme et des citoyens identifiés. J'y consacrerai un prochain article.

SIX MESURES POUR PROTÉGER LES DONNÉES CONFIÉES À L'ÉTAT

1. **La carte d'identité comme clé d'accès.** L'accès aux données sensibles de l'État se fait avec la carte d'identité électronique, validée automatiquement auprès d'un registre central des habilitations tenu par l'ANSSI ; en attendant, aucun service n'est ouvert sans un second facteur robuste, le simple code reçu par courriel n'étant plus accepté.
2. **Un délai maximal pour appliquer les correctifs critiques.** Une faille activement exploitée sur un service exposé à Internet est corrigée sous 72 heures, comme l'exige l'administration fédérale américaine ; à défaut, le service est suspendu jusqu'à sa mise à jour, et ses journaux sont analysés pour vérifier qu'il n'a pas été compromis entre-temps.
3. **Un responsable nommé pour chaque base de données.** Chaque base de données personnelles de l'État est rattachée à un responsable identifié, inscrit dans un registre consultable, qui rend compte chaque année de son niveau de sécurité.
4. **Pérenniser les pouvoirs de REACTIV.** Le pouvoir d'injonction confié à l'ANSSI devient permanent, plutôt que de créer une nouvelle structure, avec une revue d'efficacité à douze mois.

5. **Fermer les accès depuis des postes non maîtrisés.** Les applications sensibles de l'État ne sont plus accessibles depuis des ordinateurs personnels non administrés, ni pour les agents ni pour les partenaires privés qui s'y connectent ; chaque réinitialisation de mot de passe révoque toutes les sessions ouvertes.
6. **Cloisonner, superviser et publier.** Aucun outil de statistiques n'est branché directement sur une base nationale de données nominatives ; chaque application est placée sous supervision, avec des quotas de consultation ; chaque incident significatif donne lieu à un rapport public, sur le modèle du rapport DGFIP publié par l'ANSSI.

08

Que peut faire chaque citoyen ?

Redoubler de vigilance face aux messages qui citent des informations personnelles exactes, et activer la double authentification partout où elle est proposée.

Les données dérobées servent avant tout à rendre crédibles des tentatives d'escroquerie. Un message qui mentionne votre nom, votre adresse ou votre situation fiscale n'est pas une preuve d'authenticité. L'administration ne demande jamais de mot de passe ni de coordonnées bancaires par courriel, SMS ou téléphone. En cas de doute, il est préférable de se connecter soi-même au site officiel plutôt que de cliquer sur un lien reçu.

Deux gestes simples réduisent fortement le risque : ne jamais réutiliser le même mot de passe sur plusieurs sites, et privilégier une application d'authentification plutôt qu'un code reçu par courriel lorsque le choix est offert. Le dispositif public d'assistance aux victimes de cybermalveillance, cybermalveillance.gouv.fr, propose des conseils et une aide en ligne.

En refermant ce dossier, un refrain de Francis Cabrel me revient en mémoire : *Encore et encore*⁶. Tant que les correctifs attendront et que les mots de passe suffiront, la liste des fuites continuera de s'allonger.

SOURCES

- ANSSI / CERT-FR, *REACTIV — Point de situation*, septembre 2026 : cert.ssi.gouv.fr (PDF).
- ANSSI, *Rapport d'incident n° 3033/ANSSI/SDO/NP* sur les actes malveillants observés sur le système d'information de la DGFIP entre mai et août 2026, 23 septembre 2026 : cyber.gouv.fr (PDF) et [communiqué de l'ANSSI](#)
- CERT-FR, *Vulnérabilité dans Metabase*, alerte CERTFR-2026-ALE-010 : cert.ssi.gouv.fr
- CISA, *CISA Adds Three Known Exploited Vulnerabilities to Catalog*, 11 août 2026 : cisa.gov
- The Hacker News, *Metabase Zero-Day Exploited in Wild Allows Admin Access Without Authentication*, août 2026 : thehackernews.com
- ANSSI, *Cyberattaques : l'ANSSI met en place une capacité renforcée de réaction dédiée aux services de l'État*, septembre 2026 : cyber.gouv.fr
- Premier ministre, *Feuille de route des efforts prioritaires en matière de sécurité numérique de l'État 2026-2027*, 9 avril 2026 : cyber.gouv.fr
- Gouvernement, *Protection des données des Français : l'État poursuit une stratégie accélérée de sécurisation*, 2026 : info.gouv.fr
- Clubic, *99 fuites de données en deux mois, l'ANSSI dévoile la terrible ampleur du piratage des ministères français*, 1^{er} octobre 2026 : clubic.com
- Clubic, *Personne n'est à l'abri ! L'ANSSI et la Dinum victimes d'une fuite de données*, 1^{er} octobre 2026 : clubic.com
- Philippe Agnelli, brevet FR 2807247, *Système de paiement permettant de ne pas divulguer d'information bancaire sur le réseau public et quasi-public*, déposé le 28 mars 2000 : [Google Patents](#) ; extension internationale WO 01/73706 : [Google Patents](#)
- Philippe Agnelli et Roger Reynier, demande de brevet FR 2830100, *Système de paiement sécurisé entre particuliers permettant de ne pas divulguer d'information bancaire sur le réseau public et quasi public*, déposée le 24 septembre 2001 : [Google Patents](#)

NOTES

1. L'Agence nationale de la sécurité des systèmes d'information, créée en 2009, est l'autorité nationale de cybersécurité. Elle est rattachée au Secrétariat général de la défense et de la sécurité nationale, placé auprès du Premier ministre, et opère le CERT-FR, centre gouvernemental de veille et de réponse aux attaques informatiques. ↵
2. La direction interministérielle du numérique, placée sous l'autorité du Premier ministre, pilote la transformation numérique de l'État et opère des services communs aux administrations, dont ProConnect. Sa fusion avec la direction interministérielle de la transformation publique (DITP) a été annoncée le 30 avril 2026. ↵
3. ANSSI, rapport d'incident n° 3033/ANSSI/SDO/NP du 23 septembre 2026, synthèse exécutive. ↵
4. Sébastien Lecornu, Premier ministre. ↵

5. Brevet FR 2807247, déposé le 28 mars 2000, délivré en 2003 et étendu par la demande internationale WO 01/73706 ; demande FR 2830100, déposée le 24 septembre 2001 avec Roger Reynier, consacrée aux paiements entre particuliers. Les deux documents sont consultables sur Google Patents (voir les sources). [↩](#)
6. Francis Cabrel, auteur-compositeur-interprète, *Encore et encore*, chanson parue en 1985. [↩](#)

Philippe Agnelli — Ingénieur informatique, président d'Élysée Conseils, Projet 2027 — Réussir ensemble

Le raisonnement et les propositions de cet article s'appuient sur le contexte environnemental, social et économique à la date de sa rédaction. Si ce contexte évolue, l'analyse et les conclusions seront appelées à évoluer avec lui.