Cybersécurité : Focus Cybersécurité. Janvier 2026. Un début d'année sous tension temporisé par l'ambitieuse Stratégie de cybersécurité nationale ? Yannick Pech

Jacqueline Sala

L'année 2026 s'est ouverte sur une séquence particulièrement dense pour la cybersécurité. Les fuites massives de données, en particulier d'entités françaises confirment le degré élevé d'industrialisation du cybercrime, tandis que plusieurs organismes publics et grandes entreprises françaises ont subi des incidents majeurs. Dans le même temps, la multiplication des attaques sur les infrastructures critiques relance le débat sur la souveraineté numérique, la dépendance au cloud et la capacité réelle des organisations à maîtriser leurs chaînes technologiques. L'ambitieuse Stratégie de cybersécurité nationale, dévoilée le 29 janvier, viendra-t-elle contrebalancer cet état de fait et dissiper les doutes raisonnables sur la capacité des autorités politiques à traduire cette feuille de route en actes concrets ?

Vagues de fuites de données en janvier : un nouveau seuil critique atteint

Ce mois se distingue par une accumulation sans précédent de fuites de données, touchant simultanément des acteurs du commerce, de l'immobilier, du secteur associatif, de l'éducation et des services publics. Le panorama s'avère préoccupant : plusieurs dizaines de millions de personnes sont potentiellement concernées en France sur le seul premier mois de l'année. Parmi les incidents les plus marquants figurent les fuites affectant EasyCash (14 millions de clients) ; la chaine de restauration française O'Tacos (29 millions de comptes) ; plusieurs fédérations sportives nationales (FFG, FFT, FFSPT, FFvolley, FFESSM, FFTWIRL, FFME) ; la Fédération française des sapeurs-pompiers (822 449 pompiers) ; des établissements d'enseignement (IEP Paris, CNAM, Agro Paris Tech. ULille le 29/12/25), ainsi qu'un grand nombre d'acteurs du secteur immobilier le 28/01 : 11 agences dont Marteau Immobilier (du groupe Orpi, déjà attaqué le 23/01) et Trenta Immobilier, exposant adresses postales, identifiants et mots de passe, contrats, justificatifs de domicile, IBAN, pièces d'identité et autres pièces administratives sensibles. Au total, 1,2M de documents à hauteur de 500 Go de données. La diversité des organisations touchées montre que la menace ne se limite plus aux grandes entreprises technologiques, mais frappe l'ensemble du tissu économique et associatif. Cette multiplication des incidents illustre une fragilité persistante des systèmes d'information, souvent liée au facteur humain, à des erreurs de configuration cloud, à l'absence d'authentification forte ou à des infrastructures informatiques vieillissantes. Elle pose aussi la question du temps de réaction : dans de nombreux cas, les bases compromises restent accessibles plusieurs semaines avant détection, laissant aux attaquants le loisir d'exfiltrer et de revendre des volumes considérables de données ou, le plus souvent, d'en monnayer l'accès.

URSSAF, La Poste/Banque Postale : les services publics en seconde ligne

Le mois de janvier a également été marqué par plusieurs attaques visant directement des institutions publiques clés. L'URSSAF a ainsi confirmé une fuite majeure liée à la compromission d'un prestataire, exposant les données professionnelles de près de 12 millions de salariés. Si les données bancaires et les numéros de sécurité sociale n'auraient a priori pas été touchés, les informations récupérées permettent néanmoins de lancer des campagnes de phishing ciblé de grande envergure, augmentant le risque d'escroqueries voire d'usurpations d'identité. Parallèlement, le groupe La Poste, incluant La Banque Postale et Colissimo, a subi une cyberattaque d'ampleur par déni de service distribué (DDOS) dès le 1er janvier et durant plusieurs jours, entraînant l'indisponibilité temporaire de nombreux services critiques comme la livraison de colis ou ses prestations bancaires. Ces incidents, concentrés sur des infrastructures essentielles du quotidien, rappellent que la continuité de service numérique (notion de disponibilité, un des piliers de la triade de la cybersécurité avec la confidentialité et l'intégrité) est devenue un enjeu de sécurité nationale. Ces attaques soulignent une nouvelle fois l'importance du maillage entre acteurs publics et prestataires privés : une compromission indirecte peut en effet produire des effets systémiques, rendant indispensable une approche globale de la sécurité de la chaîne d'approvisionnement numérique.

Fuites industrielles et données stratégiques : un risque de sécurité physique

Au-delà des données personnelles, janvier 2026 a vu émerger plusieurs incidents mettant en jeu des données critiques à dimension stratégique et sécuritaire. Une fuite massive provenant d'un bureau d'ingénierie français (DCE Conseil) dans le BTP, les installations techniques et l'énergie a ainsi exposé des plans techniques détaillés de prisons, de bâtiments administratifs sensibles et même d'une base militaire, accompagnés d'audits de sécurité interne. Selon l'hebdomadaire Le Point, l'incident daterait de fin 2025, les pirates informatiques ayant compromis le compte cloud d'un ingénieur commercial, probablement via des identifiants volés, et exfiltré 844 Go de fichiers sensibles. Parmi ces données figuraient des plans techniques détaillés et des audits de sécurité concernant la base-école Général Lejay de l'ALAT au Cannet-des-Maures (Var), des établissements de la gendarmerie nationale et plusieurs prisons françaises, ainsi que des informations sur de grandes entreprises comme Hermès, Lidl, Sodexo, Dalkia (EDF) et Veolia. Les données volées ont été mises en vente sur BreachForums, une plateforme criminelle du darkweb, une première fois en octobre 2025 puis de nouveau en janvier 2026. Propriétaire de la base militaire compromise, l'ALAT n'aurait pas été informée de l'incident. La gendarmerie confirme s'être saisie des faits et a diligenté une enquête. Les ministères de la Justice, de l'Intérieur et des Armées ainsi que lesdites entreprises n'avaient pas répondu aux sollicitations du Point du 6 janvier, après la révélation de la fuite. Ainsi, il s'agirait d'un incident dont l'ampleur n'aurait pas été sérieusement prise en compte et pour lequel la réponse tardive des autorités dénoterait un certain flottement. Ce type d'incident démontre une nouvelle fois que, au-delà de la rentabilité financière immédiate, la cybercriminalité fusionne avec des intérêts de nature (géo)politique, en exfiltrant des informations susceptibles de fragiliser directement la sécurité physique des sites et des personnes. La circulation de ces données sur des forums clandestins accroît potentiellement le risque d'attaques ciblées, d'espionnage industriel ou d'actions malveillantes à caractère terroriste. Et corrobore l'idée d'une convergence croissante entre numérique, sécurité intérieure et défense nationale, imposant une coopération renforcée entre autorités civiles, militaires et acteurs privés. Au-delà, cela confirme que la directive NIS 2, à laquelle sans nul doute ce cabinet de conseil serait astreint, doit être traduite au plus vite dans le droit français.

Dépendance au cloud et vulnérabilité structurelle des organisations

Les nombreux incidents de janvier mettent également en lumière la

dépendance massive des organisations françaises aux services cloud, très largement hébergés sur des infrastructures étrangères, géographiquement ou à tout le moins juridiquement. Les erreurs de configuration, les compromissions de comptes administrateurs et les défauts de segmentation des accès informatiques apparaissent comme des vecteurs d'attaque récurrents. Cette dépendance soulève des interrogations majeures sur l'autonomie numérique européenne en général et la souveraineté française en particulier. Si le cloud permet agilité et performance, il concentre également les risques : une seule faille peut exposer simultanément des millions de données. Le mois de janvier confirme la nécessité d'accélérer le développement de solutions souveraines et/ou européennes, auditées et interopérables, capables d'offrir des garanties renforcées en matière de sécurité, de conformité réglementaire et de résilience opérationnelle. Les législations extraterritoriales notamment américaines ayant encore raison des efforts consentis par les autorités françaises, même avec les standards les plus aboutis à ce jour (le SecNumCloud 3.2 de l'ANSSI). C'est du moins l'avis de certains experts qui pointent du doigt les limites tant juridiques que techn(olog)iques de cette norme française visant à certifier la qualité et la sécurité des offres de service cloud.

Ultra-professionnalisation du cybercrime et industrialisation des fuites de données

Enfin, les publications régulières de données sur les forums spécialisés des data brokers* (illégaux voire légaux) et les plateformes de revente démontrent une industrialisation de plus en plus poussée du cybercrime. Les groupes malveillants structurent leurs opérations comme de véritables chaînes logistiques avec un découpage des tâches et une sous-traitance de niveau professionnel : collecte automatisée/scraping, stockage, tri, enrichissement, corrélation, revente par lots sectoriels, « positionnement marketing » via démonstrations d'échantillons. Cette professionnalisation transforme la fuite de données en marché noir structuré, où les informations personnelles deviennent une matière première stratégique pour la fraude, l'ingénierie sociale et le contournement des systèmes de sécurité. Pour les entreprises comme pour les administrations, l'enjeu n'est plus seulement la prévention, mais la capacité de détection rapide, de confinement et de communication de crise, afin de limiter l'impact réputationnel et juridique. * Les data brokers sont des courtiers en données, individus ou entreprises qui collectent, achètent et revendent des données à caractère personnel ou professionnel à des fins de profilage publicitaire et marketing. Bien que licites quoique souvent situés en zone grise (violations de la vie privée/contournement du RGPD), leurs activités et marché sont extrêmement opaques et peuvent à l'occasion être récupérés ou concurrencés par des data brokers cette fois purement illégaux, liés à la cybercriminalité.

Publication de la Stratégie nationale de cybersécurité 2026

La Stratégie nationale de cybersécurité 2026-2030 a été dévoilée le 29 janvier par Anne Le Hénanff, ministre déléguée chargée de l'Intelligence artificielle et du Numérique, au Campus Cyber régional de Nouvelle-Aquitaine à Bordeaux. Face au lourd bilan : 348 000 atteintes numériques ; hausse des cyberattaques de 74% sur cinq ans ; 43M de Français concernés par les fuites de données des deux dernières années ; 6/10 PME victimes d'une cyberattaque sont en dépôt de bilan dans les six mois, Cette stratégie vise à faire de la France une puissance cyber de premier plan, capable de protéger durablement ses citoyens, ses institutions, son économie et ses infrastructures critiques face aux cyberattaques. Elle repose sur cinq piliers déclinés en quatorze objectifs : Pilier 1 : Faire de la France le plus grand vivier de talents cyber d'Europe Développer une culture inclusive de la cybersécurité dès le plus jeune âge Investir dans tous les pans de la formation en cybersécurité Soutenir la dynamique des ressources humaines cyber au niveau européen Pilier 2 : Renforcer la résilience cyber de la nation Préparer la nation aux crises dues aux cyberattaques Rehausser le niveau global de cyber-protection Faciliter les parcours vers une meilleure cybersécurité Pilier 3 : Entraver l'expansion de la cybermenace Activer l'ensemble des leviers pour décourager les agressions cyber Mobiliser les acteurs privés dans la cyberdéfense de la nation Pilier 4 : Garder la maîtrise de la sécurité de nos fondements numériques Investir dans la sécurité des technologies numériques Soutenir la structuration d'un marché européen des produits et services de cybersécurité Maîtriser les dépendances technologiques dans le champ de la sécurité numérique Pilier 5 : Soutenir la sécurité et la stabilité du cyberespace en Europe et à l'international Promouvoir un cadre et une gouvernance internationale garantissant la sécurité du cyberespace Agir en allié et partenaire coopératif et fiable Développer une capacité de cyber-solidarité Ce document prolonge la Revue nationale stratégique 2025 et s'inscrit dans le sillage de la Revue stratégique de cyberdéfense de 2018. Au bilan, une stratégie ambitieuse qui, pour porter ses fruits et véritablement se concrétiser, devra dépasser les incantations et questionner les postures politiques jusqu'ici largement démagogiques, notamment sur le plan des dépendances technologiques et de la souveraineté numérique. La (cyber)puissance ne se décrétant pas, mais se traduisant en actes.

Perspectives

Janvier 2026 confirme que la cybersécurité se situe dans un état de tension permanent. L'explosion des fuites de données, les attaques contre les services publics et des entreprises de toutes dimensions, la compromission de données stratégiques confirment que la menace est structurelle, continue et protéiforme. Face à ce constat, trois priorités émergent : renforcer la sécurité des chaînes de sous-traitance, accélérer la montée en maturité cyber des organisations de taille intermédiaire, et investir massivement dans une infrastructure numérique souveraine et résiliente. À défaut, la répétition de ces incidents risque d'éroder durablement la confiance des citoyens dans les services numériques et fragiliser une économie déjà à la peine.

Résumé

Explosion des fuites de données : janvier 2026 bat des records, avec des dizaines de millions de personnes potentiellement concernées, à travers des acteurs publics, privés et associatifs. Services publics ciblés : URSSAF, La Poste et Banque Postale ont subi des attaques préjudiciables au principe de disponibilité d'accès aux données et services liés au numérique (garanties de continuité numérique, résilience). Données stratégico-sécuritaires exposées : plans de prisons, audits internes et infrastructures militaires sensibles divulgués. Dépendance au cloud : fragilité structurelle des organisations françaises, maillées dans des entrelacs de dépendances à des infrastructures techn(olog)iques et des législations étrangères extraterritoriales. Industrialisation du cybercrime : professionnalisation avancée des filières de vol, recel ou revente de données. Stratégie de cybersécurité nationale : un document ambitieux qui devra se confronter aux décisions souvent contradictoires et dissonantes des autorités politiques

Sources principales utilisées

Bonjour la fuite – Fuites de données – janvier 2026 https://bonjourlafuite.eu.org ZATAZ – Alertes et analyses cybersécurité – janvier 2026 https://www.zataz.com Le Monde Informatique – Cyberattaques et incidents majeurs – janvier 2026 https://www.lemondeinformatique.fr Le Point – Fuite de données insoupçonnée issue d'un bureau d'études https://www.lepoint.fr/high-tech-internet/base-militaire-gendarmerie-prisons-ce-que-revele-une-fuite-de-donnees-passee-sous-les-radars-C2Z2WVUMCREBBLYOHCPGEAXVII/ 01net – Fuite de données issue d'un cabinet de conseil https://www.01net.com/actualites/fuite-donnees-devoile-plans-plusieurs-prisons-base-militaire-francaise.html LinkedIn – éléments de débats et opinions exprimées par des experts en cybersécurité (sujet de la souveraineté numérique) Secrétariat général de la défense et de la sécurité nationales (SGDSN) – 29 janvier 2026 https://www.sgdsn.gouv.fr/publications/strategie-nationale-de-cybersecurite-2026-2030 Cybernetica.fr – janvier 2026

Veillecyber.fr – janvier 2026

A propos de l'auteur

Yannick PECH est docteur en sciences de l'information-communication, spécialiste du renseignement et de la cybersécurité, certifié pentester junior. Yannick PECH Yannick PECH est docteur en sciences de l'information-communication, spécialiste du renseignement et de la cybersécurité, détenteur d'une certification de Pentester junior (eJPT) et de la certification EBIOS Risk Manager de l'ANSSI. Chargé de cours en géopolitique, intelligence économique, sécurité numérique et OSINT dans le supérieur privé et public, chercheur associé au CEREGE de l'IAE de Poitiers, ancien veilleur-analyste à la Compagnie européenne d'intelligence stratégique (CEIS), consultant-analyste au CRR-FR (OTAN-France) et réserviste opérationnel-spécialiste de l'armée de Terre, il est désormais officier de la Réserve citoyenne de cyberdéfense au sein de la gendarmerie d'Occitanie. Il prépare actuellement la certification ISO-27001 (GRC/SMSI).

E-mail : jsala@veillemag.com
Url : https://www.veillemag.com