La souveraineté numérique en 2026 entre la théorie et le quotidien ?
La souveraineté numérique en 2026 entre la théorie et le quotidien ?
 Bernard Sfez - 2026-04-29 08:49

Entre notre premier article en février et aujourd'hui, il s'est passé plus de choses en matière de souveraineté numérique que durant les cinq années précédentes. La France annonce la migration de 2,5 millions de postes vers Linux, l'Europe cible les algorithmes de recommandation, 80 000 agents de l'Assurance maladie basculent vers des outils souverains. Mais dans le même temps, les fuites de données explosent : 19 millions de Français exposés par le piratage de l'ANTS, la France devenue deuxième pays le plus touché au monde, trois comptes compromis chaque seconde. Les gouvernements bougent, tant mieux. Mais que font ceux qui n'ont ni DSI ni budget ministériel ?

Ce quatrième volet vous propose un tour d'horizon de ce qui a changé en quatre mois, un état des lieux des menaces qui s'accumulent, et surtout une checklist d'actions concrètes, classées par temps et par effort, que chacun peut entreprendre pour commencer à protéger ses données et celles de ses clients. Des mesures simples, accessibles, avec vos moyens et à votre échelle.

Dans un précédent article, nous avons cartographié l'étendue de notre dépendance numérique. Dans un deuxième, nous avons examiné ce que l'État faisait, ou ne faisait pas, pour nous en sortir. Et dans notre dernier article, nous avons posé les bases concrètes d'une infrastructure souveraine.

Ce quatrième volet change de registre. Nous commençons à examiner ce que nous pouvons faire, nous, au quotidien. Les particuliers, les PME, les associations, les collectivités locales, les indépendants. Pour protéger nos données, celles de vos partenaires et clients, sécuriser notre activité et respecter les lois et réglementations qui s'appliquent désormais à tous.

Mais d'abord, un tour d'horizon s'impose. Entre notre premier article en février et aujourd'hui, le paysage a bougé. En bien et en moins bien. Côté avancées, de nouvelles lois, des migrations sans précédent et un signal politique fort. Côté menaces, une explosion des fuites de données massives et l'arrivée d'une nouvelle génération d'intelligence artificielle capable de découvrir des milliers de failles de sécurité en quelques heures, au point que son éditeur a préféré en reporter la mise à disposition publique. Ce qui servira demain à nous protéger sert déjà aujourd'hui à automatiser les attaques.

Après ce rapide tour d'horizon, nous reviendrons à la question qui devient incontournable pour

tous ceux qui ne sont ni ministère ni multinationale : et nous, on fait quoi ?

Ce qui a changé en quatre mois

Les Etats passent aux actes

Le 8 avril 2026, la DINUM a organisé un séminaire interministériel sans précédent réunissant ministères, opérateurs publics et acteurs privés autour d'un objectif unique : réduire les dépendances numériques extra-européennes. Ce n'est pas le premier discours sur le sujet. Mais cette fois, les annonces sont assorties de calendriers et d'obligations.

La DINUM elle-même quitte Windows pour Linux. La Caisse nationale d'Assurance maladie migre ses 80 000 agents vers des outils souverains (Tchap pour la messagerie, Visio pour les réunions, FranceTransfert pour l'échange de documents). La plateforme des données de santé, jusqu'ici hébergée chez Microsoft Azure, doit basculer vers une solution souveraine d'ici fin 2026. Et chaque ministère doit présenter avant l'automne une feuille de route couvrant huit catégories : postes de travail, outils collaboratifs, antivirus, intelligence artificielle, bases de données, cloud, virtualisation et équipements réseau.

La France n'est pas seule. Le Land de Schleswig-Holstein en Allemagne a déjà migré 80 % de ses 30 000 postes de travail et économisé 15 millions d'euros en licences sur la seule année 2026. La GendBuntu française, souvent citée en exemple, tourne désormais sur plus de 103 000 postes avec une réduction du coût total de possession estimée à 40 %.

Faut-il y croire cette fois ? L'histoire incite à la prudence. Munich avait tenté une migration comparable dans les années 2000 avant de revenir à Microsoft sous pression. Mais le contexte de 2026 est radicalement différent. Les tensions géopolitiques avec les États-Unis ont rendu la dépendance numérique visible à tous. Le Cloud Act n'est plus un sujet de spécialistes, c'est un argument au Sénat. Et surtout, la pression ne vient plus d'un seul pays : c'est toute l'Europe qui bouge.

L'Europe légifère

En février 2026, la Commission européenne a publié un avis préliminaire estimant que TikTok viole le DSA à cause de ses fonctionnalités addictives et de son système de recommandation hautement personnalisé. C'est la première fois qu'une institution démocratique cible juridiquement un algorithme de recommandation.

En France, un projet de loi du 26 janvier 2026 visant à protéger les mineurs ajoute un article qui change la donne : les algorithmes de recommandation pourront désormais engager la responsabilité éditoriale de leur fournisseur. Autrement dit, si une IA de recommandation amplifie massivement de la désinformation ou du harcèlement, l'entreprise qui la conçoit pourrait être traitée juridiquement comme un rédacteur en chef.

La directive NIS2, entrée en vigueur, impose de nouvelles obligations de cybersécurité à un périmètre élargi d'organisations, y compris des PME et des collectivités qui n'étaient jusqu'ici pas concernées. Et le Digital Markets Act (DMA) ouvre la voie à l'interopérabilité des plateformes, avec à terme la possibilité de consulter les contenus d'une plateforme depuis une autre application, brisant le verrouillage des écosystèmes fermés.

Les fuites de données explosent

Pendant que les institutions construisent, les données fuient. Et le rythme s'accélère de manière alarmante. Depuis le début de l'année, la France subit en moyenne plusieurs incidents majeurs par semaine, un rythme sans précédent qui a fait de ce premier trimestre le plus lourd jamais enregistré.

Le dernier (publique...) en date au moment où nous écrivons : le 15 avril 2026, l'ANTS (l'agence qui gère vos passeports, permis de conduire et cartes grises) a été piratée via une faille qualifiée de « vraiment stupide » par le hacker lui-même. Il suffisait de modifier un chiffre dans une requête pour accéder aux données d'un autre citoyen. Jusqu'à 19 millions d'enregistrements compromis. Ce type de faille (IDOR) est une erreur de programmation élémentaire, enseignée en première année de formation en développement web. Sa présence sur un portail régalien gérant les titres d'identité de millions de Français démontre à elle seule l'importance de procéder à des audits de sécurité externes et indépendants, régulièrement. La réponse de l'ANTS aux utilisateurs, à la hauteur de cette incompétence : « Vous n'avez aucune démarche à accomplir. » Merci bien !

Ce n'est pas un cas isolé. En février 2026, un attaquant a accédé au fichier national des comptes bancaires (FICOBA) pendant 16 jours via les identifiants usurpés d'un fonctionnaire. Cegedim Santé a exposé les données de 15 millions de patients. L'OFII a vu fuiter 2,1 millions de dossiers d'étrangers. Alinto a laissé échapper 40 millions de métadonnées email touchant L'Oréal, Renault, Carrefour et Hermès. Et la liste continue : Crous, fédérations sportives, Parcoursup, Enseignement catholique, Basic-Fit...

Au total, la France est devenue le deuxième pays le plus touché au monde au premier trimestre 2026, avec 23,5 millions de comptes compromis, soit une hausse de 108 % par rapport au trimestre précédent.

Et ce ne sont que les grandes fuites, celles qui font la presse. Des PME ferment après un ransomware sans que personne n'en parle : Clestra Hauserman en redressement judiciaire, Camaïeu en liquidation accélérée, Lise Charmel paralysée pendant des mois. Pour une petite structure sans grosse réserve de trésorerie, quelques semaines d'arrêt suffisent pour fermer la boite.

Le problème le plus inquiétant est le croisement des données issues de multiples fuites. Une fuite vous donne un numéro de sécurité sociale. Une autre complète avec l'historique professionnel. Une troisième ajoute les coordonnées bancaires. Séparément, ces informations sont déjà exploitables. Combinées, et c'est désormais possible grâce aux nouveaux outils d'intelligence artificielle capables de recouper et structurer des millions d'enregistrements en quelques heures, elles permettent une usurpation d'identité complète.

Et vous dans tout ça ?



> *La réglementation avance. Les grandes institutions bougent. Les ministères ont des feuilles de route et des budgets. Les multinationales ont des DSI et des cabinets de conseil. Pendant ce temps, les fuites de données frappent tout le monde sans distinction.*
>
> *Et vous, PME, association, collectivité locale, indépendant, avec ou sans responsable informatique, avec ou sans budget dédié, vous faites quoi ?*

La bonne nouvelle, c'est que vous n'avez pas besoin d'être un expert pour commencer. Vous n'avez pas non plus besoin de tout faire d'un coup ni de tout faire seul. La plupart des actions décrites ci-dessous sont accessibles, progressives et souvent gratuites. Certaines prennent une heure. D'autres demandent un week-end. Quelques-unes nécessiteront un plan structuré et peut-être un regard extérieur pour éviter les faux départs. C'est aussi l'occasion de commencer à responsabiliser votre équipe sur ces sujets. Et si le temps vous manque ou si la démarche vous semble trop perturbante pour votre activité, des prestataires spécialisés peuvent établir un plan raisonnable, adapté à votre échelle, c'est d'ailleurs une part importante de ce que nous faisons. Mais l'essentiel, c'est de commencer, car en matière de protection des données, il est déjà tard.

Nous avons organisé ce qui suit en checklist, comme une liste de courses. Vous n'êtes pas obligé de tout prendre en un seul passage. Parcourez les rayons, repérez ce qui correspond à votre situation et commencez par ce qui vous semble le plus urgent ou le plus simple. Le reste viendra avec le temps, à condition de suivre un peu l'actualité et de lire de temps en temps des articles comme celui que vous êtes en train de parcourir.

Ce qui prend une heure+ (et ne coûte rien)

Vérifiez vos mots de passe

Allez sur Have I Been Pwned et entrez les adresses email que vous utilisez au quotidien. Vous découvrirez probablement que plusieurs de vos adresses figurent déjà dans des fuites de données. Si c'est le cas, changez immédiatement les mots de passe concernés. Et si vous utilisez le même mot de passe sur plusieurs services, c'est le moment d'arrêter. Un seul compte compromis ouvre la porte à tous les autres.

Peut-on faire confiance à ce site ?
Have I Been Pwned a été créé en 2013 par Troy Hunt, un expert en sécurité australien reconnu qui a notamment témoigné devant le Congrès américain sur les fuites de données. Le service est entièrement open source depuis 2021, son code est vérifiable sur GitHub. Les gouvernements d'Australie, du Royaume-Uni et d'Espagne l'utilisent officiellement pour surveiller leurs domaines. Le FBI y injecte directement les identifiants compromis qu'il découvre dans ses enquêtes. Vous n'entrez qu'une adresse email, jamais un mot de passe. Par honnêteté, signalons que Troy Hunt lui-même a été victime d'un phishing en mars 2025, preuve que personne n'est infaillible, mais il a publié l'incident sur sa propre plateforme, ce qui en dit long sur sa transparence.

Installez un gestionnaire de mots de passe

KeePassXC est open source, gratuit, et stocke vos mots de passe en local sur votre machine, rien ne sort de chez vous. Bitwarden est une alternative open source si vous avez besoin de synchroniser entre plusieurs appareils. Il est auto-hébergeable, "in-house", et c'est le type de mise en place qu'un prestataire comme OpenSource Solutions peut installer et configurer pour vous. Les solutions propriétaires comme 1Password offrent une intégration navigateur et mobile plus fluide, c'est indéniable. Mais posez-vous la question : où sont stockés vos mots de passe ? Chez 1Password, la réponse est sur des serveurs américains, chez AWS, soumis au Cloud Act. Autrement dit, la clé de tous vos comptes est hébergée dans la juridiction exacte dont cet article vous invite à vous émanciper. C'est un choix à faire en connaissance de cause, pas un détail. Dans tous les cas, n'importe lequel de ces outils vaut infiniment mieux que le même mot de passe partout, le fichier Excel « mdp.xlsx » sur le bureau, ou le post-it collé sur l'écran que vous êtes peut-être en train de regarder. Si vous êtes plusieurs dans votre structure, c'est le premier outil à déployer collectivement.

Et pour les accès critiques de l'entreprise ?
Pour les mots de passe partagés d'une structure (accès serveurs, comptes administrateurs, clés API, identifiants fournisseurs), la question est différente. Il ne s'agit plus de confort personnel mais de continuité d'activité. Que se passe-t-il si la seule personne qui connaît le mot de passe root est absente ? Dans une grande entreprise d'armement avec laquelle nous avons travaillé, la solution est radicalement low-tech : une enveloppe scellée dans un coffre-fort physique, mise à jour à chaque changement de mot de passe. Ce n'est pas élégant, mais c'est résilient, hors réseau, et imperméable à toute cyberattaque. Pour les structures plus modestes, des solutions de gestion d'accès partagés existent et peuvent être hébergées sur votre propre infrastructure.

Changez de navigateur et de moteur de recherche.

Firefox (Mozilla, fondation à but non lucratif) plutôt que Chrome (Google). Brave est une alternative intéressante avec un blocage natif des trackers, mais reste une entreprise américaine.

Pour le moteur de recherche, Qwant (français) ou DuckDuckGo plutôt que Google Search. Ce sont des gestes simples qui réduisent immédiatement la quantité de données personnelles collectées sur votre navigation, celle de vos collaborateurs et celle de vos clients quand ils visitent vos locaux et utilisent votre Wi-Fi. On sait que changer ses habitudes n'enthousiasme personne. Mais ces navigateurs sont plus rapides, affichent moins de publicités, consomment moins de mémoire et ne vous suivent pas à la trace. Au bout d'une semaine, personne ne revient en arrière.

Ce qui prend un week-end (et change déjà beaucoup)

Jitsi pour vos réunions en ligne

Chaque réunion sur Teams ou Zoom transite par des serveurs américains. Les métadonnées de vos appels (qui parle à qui, quand, combien de temps, depuis où) sont collectées et stockées sous juridiction américaine. Et les contenus eux-mêmes ne sont pas épargnés : les enregistrements, les transcriptions automatiques et les résumés générés par l'IA intégrée à ces plateformes alimentent des modèles d'apprentissage et constituent une source de renseignement dont vous n'avez aucun contrôle. Pour des réunions internes sensibles, des échanges avec des clients ou des discussions stratégiques, c'est un risque que beaucoup d'organisations sous-estiment. Avant de renouveler vos licences, essayez Jitsi Meet. Open source, chiffré, utilisable sans compte ni installation, un simple lien dans le navigateur suffit. Envoyez le lien à vos prochains interlocuteurs et observez leur réaction. Il y a de fortes chances qu'ils ne voient aucune différence. L'État français lui-même a décidé de bannir Teams, Zoom et Google Meet de ses services pour leur substituer Visio, sa propre solution de visioconférence open source et souveraine, qui équipera ses 2,5 millions d'agents d'ici 2027. La preuve, s'il en fallait une, qu'une alternative libre tient la route à grande échelle.

Passez votre analytique web sur Matomo

Si votre site utilise Google Analytics, chaque visite de vos clients, prospects ou administrés génère des données qui sont envoyées à Google, traitées aux États-Unis et potentiellement exploitées à des fins publicitaires. Ce n'est pas seulement un problème de principe : depuis l'invalidation du Privacy Shield, plusieurs autorités européennes de protection des données ont jugé Google Analytics non conforme au RGPD_. En continuant à l'utiliser, vous exposez votre organisation à un risque juridique réel. Matomo (français, open source) fait le même travail, est conforme RGPD par conception et peut être hébergé sur votre propre serveur. Les données de vos visiteurs restent chez vous, point. La migration consiste à remplacer un bout de code sur votre site. C'est l'affaire d'une demi-journée si vous ne connaissez pas, sans doute moins si vous avez un profil technique, et c'est un service que nous déployons régulièrement.

Vérifiez votre nom de domaine et votre fournisseur email

Connectez-vous à l'interface de votre registrar et vérifiez deux choses. D'abord, que le domaine est bien enregistré à votre nom, pas à celui d'un ancien prestataire qui pourrait le conserver en cas de litige. Ensuite, que le registrar lui-même est européen. Le site European Alternatives maintient une liste de registrars européens accrédités. Si vous ne savez pas ce qu'est un registrar ou si vous ne savez pas où vous connecter, c'est déjà une information importante sur votre niveau de dépendance, et exactement le type de question qu'un accompagnement extérieur peut démêler en quelques minutes. Profitez-en pour vérifier qui gère réellement vos emails. Si vos adresses professionnelles passent par Gmail ou Outlook/Exchange, chaque message envoyé et reçu, contrats, devis, données clients, mots de passe réinitialisés, transite et est stocké chez Google ou Microsoft. Votre nom de domaine et vos emails sont les deux actifs numériques les

plus critiques de votre organisation. Ce sont aussi les premiers à reprendre en main, et nous détaillerons comment dans un prochain article consacré à la messagerie.

Faites l'inventaire de vos services en ligne

Commencez par lister les outils que votre structure utilise au quotidien. Pour chacun, posez trois questions. Où sont hébergées les données ? Sous quelle juridiction ? Et si ce service disparaît demain, est-ce que je peux récupérer mes données dans un format exploitable ? Si la réponse est non ou si vous ne savez pas, vous tenez votre première priorité pour la suite. Si votre structure est plus grande ou si vos outils sont nombreux, cet exercice devient un véritable audit qui mérite d'être structuré, nous y revenons dans la section suivante. Dans les deux cas, cet inventaire réserve des surprises, et il est souvent plus efficace quand il est mené avec un regard extérieur qui sait quelles questions poser.

Sensibilisez vos collaborateurs

Réunissez vos équipes une heure et partagez avec eux ce que vous avez appris. Les résultats de "Have I Been Pwned" sur les adresses de l'entreprise, la liste des outils et leur juridiction, les chiffres sur les fuites de données, etc. Pas pour faire peur, pour responsabiliser. La sécurité et la souveraineté numérique ne sont pas des sujets informatiques, ce sont des sujets collectifs. Et c'est souvent cette prise de conscience partagée qui déclenche le mouvement. Présentez ces informations sous une forme que vos collaborateurs pourront reproduire chez eux, avec leur famille. Les bonnes pratiques numériques ne s'arrêtent pas à la porte du bureau, et si vos équipes ont des adolescents à la maison, vous gagnerez des alliés inattendus.

Ce qui demande un plan (et probablement un coup de main)

Les actions précédentes sont des gestes individuels. Celles qui suivent touchent à l'infrastructure et à l'organisation de votre structure. Elles nécessitent une réflexion en amont, un calendrier réaliste et souvent un accompagnement. C'est ici que l'on passe du geste citoyen à la décision stratégique.

Faites un véritable audit de dépendance

Nous avons détaillé la méthode dans notre précédent article. Cartographier chaque couche (matériel, systèmes d'exploitation, applications, services cloud, shadow IT), identifier les juridictions et examiner les contrats. Si vous avez fait l'inventaire rapide du week-end, vous savez déjà où ça fait mal. L'audit structuré va plus loin : il chiffre les risques, identifie les dépendances cachées et produit une feuille de route priorisée. C'est le point de départ de tout accompagnement sérieux.

Reprenez le contrôle de vos emails

Reprenez le contrôle de vos emails. Si l'inventaire du week-end a confirmé que vos emails transitent par des serveurs américains, c'est le chantier prioritaire. Transférer votre domaine chez un registrar européen, pointer vos MX vers un serveur que vous maîtrisez, déployer une solution de messagerie souveraine. C'est un projet de quelques jours, pas de quelques mois, et nous consacrerons un article entier aux solutions disponibles. Si vous êtes dans l'urgence, contactez-nous.

Hébergez vos données sur votre propre serveur

Comme nous l'avons montré dans notre article précédent, un serveur performant et adapté à une PME se monte pour a peu près de 2000 euros de matériel, et il s'amortit en quelques mois face

aux abonnements cloud. Hébergé dans vos locaux ou chez un prestataire européen, administré via des outils open source comme Virtualmin et Webmin, il devient le socle sur lequel reposent vos emails, vos fichiers, vos sauvegardes et vos applications métier. C'est une des briques que nous déployons le plus fréquemment.

Revoyez vos contrats

Chaque prestataire identifié dans votre audit est lié à vous par un contrat que vous avez probablement signé sans le lire en détail. Vérifiez la clause de réversibilité (pouvez-vous récupérer vos données dans un format exploitable ?), la propriété des données (le prestataire s'interdit-il de les exploiter ?), la juridiction applicable (quel tribunal en cas de litige ?) et les conditions de résiliation (y a-t-il des pénalités, un préavis, une suppression automatique ?). Ce travail nécessite un regard juridique. Si vous n'avez pas d'avocat spécialisé en droit du numérique, c'est le moment d'en consulter un. Nous travaillons en partenariat avec des cabinets compétents sur ces sujets et pouvons vous orienter.

Ce qui demande du courage (et du temps)

Les chantiers précédents touchent à l'infrastructure. Ceux qui suivent touchent aux habitudes. Et c'est là que ça pique.

Migrez votre bureautique

C'est le sujet qui cristallise le plus de résistance. Après des années sur Word, Excel et PowerPoint, demander à une équipe de passer à LibreOffice ou OnlyOffice provoque des réactions épidermiques. Pourtant, pour 90 % des usages quotidiens, la transition est transparente. Le vrai obstacle n'est pas technique, il est culturel. Treize ans de scolarité sur les outils Microsoft, ça laisse des réflexes. La clé c'est l'accompagnement : pas une formation de deux heures un vendredi après-midi, mais une présence dans la durée, quelqu'un qui répond aux questions quand elles se posent, dans le contexte réel du travail. Nous détaillerons ces approches, techniques et pédagogiques, dans un article dédié.

Passez à la collaboration souveraine

Google Drive, SharePoint, Dropbox, Notion, Slack, Trello, Salesforce... Beaucoup d'organisations empilent une demi-douzaine de services américains pour collaborer. Des alternatives existent. Nextcloud pour le stockage et le partage de fichiers. Tiki Wiki pour ceux qui veulent aller plus loin : wiki, gestion de projet, CRM, formulaires, workflows et même la messagerie intégrée via Cypht, le tout dans une seule plateforme hébergée chez vous. L'avantage d'une solution tout-en-un, c'est un seul serveur à sécuriser, un seul ensemble de données à gouverner, une seule migration au lieu de six. Nous y consacrerons également un article complet.

Le poste de travail : Linux ou pas

Soyons honnêtes. Le choix du système d'exploitation sur les postes de travail est le sujet le plus sensible de toute la démarche. Linux est la seule option pleinement souveraine. Ubuntu ou Linux Mint pour la facilité, Fedora pour les environnements professionnels structurés. La Gendarmerie nationale fait tourner plus de 103 000 postes sous GendBuntu et l'État vient d'annoncer la migration de la DINUM. Mais la réalité du terrain, c'est que certains métiers dépendent de logiciels qui n'existent pas sous Linux. Graphistes sous Adobe, comptables avec des logiciels certifiés, ingénieurs en CAO. J'utilise moi-même macOS au quotidien. Le reconnaître ne discrédite pas la démarche : cela montre qu'on vit dans le monde réel. L'essentiel est de protéger ce qui compte le plus : le serveur, les données, les emails, les outils collaboratifs. Un poste macOS ou

Windows qui se connecte à une infrastructure souveraine est déjà à 80 % indépendant dans ses usages. Commencez par le serveur. Le poste de travail viendra, ou pas, selon vos contraintes réelles.

Le mobile : accepter les limites

iOS et Android se partagent 99 % du marché. Il n'existe pas d'alternative grand public. Mais vous pouvez limiter les dégâts : Signal plutôt que WhatsApp, Nextcloud plutôt que iCloud ou Google Drive, Firefox plutôt que Chrome, un gestionnaire de mots de passe local plutôt que le trousseau Google. Ce n'est pas une solution parfaite, mais c'est une réduction significative de votre surface d'exposition. Et surtout, appliquez à vos appareils mobiles les mêmes règles qu'à vos postes de travail : pas de données professionnelles sensibles sur un téléphone personnel non sécurisé. En mars 2026, l'application de jogging Strava a révélé la position exacte du porte-avions Charles de Gaulle en Méditerranée. Un officier qui faisait son footing avec un profil public. Pas de piratage, pas de cyberattaque, juste une application de fitness et un réglage de confidentialité par défaut. Votre organisation n'est probablement pas un porte-avions, mais le mécanisme est le même.

Protégez ce que vous avez repris

Reprendre le contrôle de votre infrastructure sans la protéger, c'est déménager dans une maison neuve en laissant la porte ouverte. Les sections précédentes parlent de souveraineté. Celle-ci parle de survie. Et c'est un métier.

Comme nous l'avons détaillé dans notre précédent article et rappelé plus haut avec les chiffres alarmants de ce début 2026, les attaques sont automatisées, continues et ne font pas de distinction entre une multinationale et une PME. La réponse passe par trois piliers indissociables : une supervision en temps réel qui vous alerte avant qu'un incident ne devienne une crise, un filtrage géographique des accès qui élimine le bruit et les tentatives de pénétrations avant même qu'elles n'atteignent vos accès serveur, et une sauvegarde offsite régulièrement testée parce qu'une sauvegarde qui n'a jamais été vérifiée n'est qu'un espoir. Ce n'est pas le type de chantier qu'on improvise un dimanche. C'est un ensemble cohérent qui se conçoit, se déploie et se maintient avec un prestataire qui connaît votre infrastructure et la surveille dans la durée.

Et demain, protéger vos données et votre métier face à l'IA

Il y a un sujet que nous n'avons fait qu'effleurer et qui mérite un article entier. Combien de vos collaborateurs utilisent ChatGPT, Copilot ou Gemini avec des données clients, des documents internes ou des informations stratégiques ? Chaque requête alimente des modèles entraînés sur vos données, hébergés sous juridiction américaine, sans que vous ayez aucun contrôle sur leur usage ultérieur. Et ce n'est qu'une face du problème : vos contenus publics, vos documentations, votre savoir-faire métier sont déjà aspirés par des IA qui s'en nourrissent pour entraîner des modèles qui serviront peut-être vos concurrents. Des alternatives souveraines existent et mûrissent rapidement. Des modèles open source comme Mistral ou LLaMA peuvent tourner sur vos propres serveurs, en local, sans qu'aucune donnée ne quitte votre infrastructure. Nous y consacrerons un prochain article.

La suite vous appartient

Entre les annonces gouvernementales, les nouvelles réglementations et l'explosion des cyberattaques, 2026 marque un tournant. La souveraineté numérique n'est plus un débat de spécialistes, c'est un enjeu quotidien pour toutes les organisations, quelle que soit leur taille.

Ce que nous avons partagé dans cet article, ce ne sont pas des solutions miracles. Ce sont des premiers pas que n'importe quelle structure peut entreprendre à son rythme. Certains prennent une heure et d'autres demandent un plan et un accompagnement. Tous contribuent à réduire votre exposition et à renforcer votre indépendance.
Dans les prochains articles, nous détaillerons chaque brique avec la même approche concrète :

- La messagerie : reprendre le contrôle de vos emails, de la migration DNS au déploiement d'une solution souveraine avec Cypht et Tiki Wiki
- La bureautique : méthodes techniques et pédagogiques pour une transition en douceur vers LibreOffice ou OnlyOffice
- La collaboration et le stockage : Nextcloud, Tiki Wiki et comment remplacer une demi-douzaine de SaaS américains par une plateforme que vous maîtrisez
- L'analytique et le web : Matomo, hébergement souverain, SEO sans Google
- La cybersécurité au quotidien : hygiène numérique, bonnes pratiques utilisateurs, ce que chacun peut faire
- L'IA souveraine : protéger vos données métier et déployer une intelligence artificielle locale sur votre infrastructure
- Le particulier : ce que chacun peut faire chez soi, pour soi et pour sa famille

Si vous ne voulez pas manquer ces publications, abonnez-vous à notre infolettre. Pas de spam, pas de rythme effréné, juste un signal quand un nouvel article sort ou quand l'actualité de la souveraineté numérique le justifie. Et si après cette lecture vous avez identifié des urgences ou si vous ne savez tout simplement pas par où commencer, c'est exactement pour ça que nous sommes là.