Emails et visio : reprendre le contrôle de votre communication

Emails et visio : reprendre le contrôle de votre communication

Bernard Sfez - 2026-06-23 19:44

Vos emails et vos réunions concentrent l'essentiel de vos données sensibles : contrats, devis, échanges stratégiques, fichiers clients. C'est aussi là que se niche votre plus grande exposition, et paradoxalement le chantier le plus rentable à reprendre en main. Dans ce nouveau volet de notre série sur la souveraineté numérique, nous passons de la théorie à la pratique.

Car le constat est sans appel. Chaque courriel, chaque réunion qui transite par un service américain ou tenue sur une plateforme étrangère relève d'une juridiction qui n'est pas la vôtre. Pourtant, reprendre la main n'a rien d'un chantier insurmontable. Voici, étape par étape, comment retrouver la maîtrise de votre communication, du geste simple à la portée de tous jusqu'aux solutions qui gardent réellement vos données sous contrôle.

Dans cette série, nous avons d'abord cartographié l'étendue de notre dépendance numérique, puis examiné ce que l'État fait, ou ne fait pas, pour nous en sortir, avant de poser les bases concrètes d'une infrastructure souveraine. Dans notre dernier volet, nous avons quitté la théorie pour le quotidien et promis de passer à l'action, brique par brique.

Voici la première brique. Et ce n'est pas un hasard si nous commençons par la communication : c'est le chantier dont le rapport effort sur souveraineté récupérée est le plus avantageux. C'est par là qu'il faut commencer, parce que c'est là qu'on gagne le plus, et le plus vite. Pas besoin de tout révolutionner du jour au lendemain. Il suffit de savoir où poser le premier geste, puis le suivant.

## L'email : votre actif le plus critique

L'email est le nerf de la guerre. C'est par là que transitent les contrats, les données clients, les échanges stratégiques et les réinitialisations de mots de passe. C’est aussi, trop souvent, la porte d’entrée de l’usurpation d’identité. Le diagnostic est sévère, mais le remède est à votre portée : c'est la brique la plus rentable à reprendre en main. Le rapport entre l'effort fourni et la souveraineté récupérée y est imbattable.

## Premier geste : reprenez votre nom de domaine

Une règle de base avant tout le reste : vous devez maîtriser votre propre nom de domaine, car il porte vos adresses et l'acheminement de votre courrier. Commencez donc par le socle, votre nom de domaine et vos enregistrements DNS.

Si votre registrar actuel est une entreprise américaine soumise au Cloud Act, transférez votre domaine chez un prestataire européen relevant exclusivement du droit européen. Parmi les registrars européens accrédités ICANN, on trouve OVHcloud, Gandi, Netim ou Scaleway en France, Infomaniak en Suisse, IONOS en Allemagne, pour ne citer que les plus connus. Le site European Alternatives maintient une liste à jour de fournisseurs européens par catégorie.

Une fois le domaine sécurisé, il suffit de modifier vos enregistrements MX pour les faire pointer vers un serveur que vous maîtrisez. Le changement est transparent pour vos utilisateurs et ne prend que quelques heures.

## Quelles alternatives à Microsoft 365 ou Google Workspace pour les emails ?

Pour le serveur de messagerie lui-même, pas besoin d'usine à gaz. Un serveur Linux équipé de Virtualmin, un logiciel de gestion de serveur et d'hébergement souverain internet, fournit une infrastructure email complète et éprouvée : comptes IMAP et SMTP, filtrage antispam, authentification SPF, DKIM et DMARC, certificats SSL, le tout sur une machine que vous contrôlez en interne ou que vous hébergez chez un prestataire européen. C'est une base solide, sobre, et c'est l'une des briques que nous déployons et configurons le plus fréquemment pour nos clients, à travers notre service de messagerie professionnelle souveraine infogérée, une vraie alternative à Microsoft 365 / Google Workspace.

Côté accès, vous n'êtes enfermé nulle part. Tout repose sur des standards ouverts (IMAP, SMTP, CalDAV, CardDAV), ce qui vous laisse libre du client de messagerie. Un webmail accessible depuis n'importe quel navigateur, comme Roundcube ou le webmail intégré à Tiki Wiki, un CMS Open source, pour consulter ses messages depuis n'importe quel poste. Une application dédiée, comme Thunderbird, Evolution ou les clients natifs de Windows, macOS, iOS et Android, pour qui préfère travailler hors du navigateur. Chacun choisit son outil ; vos emails, contacts et agendas restent les mêmes d'un appareil à l'autre, accessibles partout.

Pour la plupart des indépendants, PME, associations et collectivités, ce niveau suffit amplement. Vous récupérez le contrôle de vos communications, vos données restent sous juridiction européenne, et vous n'avez plus à dépendre du bon vouloir d'un géant américain.

## Pour aller plus loin : quand l'email devient un outil métier

Reprendre le contrôle de sa messagerie professionnelle, c'est déjà beaucoup. Mais pour les organisations qui veulent aller plus loin, le logiciel libre ouvre une porte que les solutions propriétaires gardent fermée : transformer l'email en véritable donnée métier.

C'est la promesse de Cypht, un client webmail open source qui, intégré à Tiki Wiki, cesse d'être une simple boîte de réception pour devenir un outil de gestion de la communication. Le principe a été présenté au FOSDEM 2025, la plus grande conférence européenne du logiciel libre, sous un titre éloquent : « Email as a first-class citizen ». Et ce n'est pas un projet isolé ni expérimental, il bénéficie d'une collaboration active entre les équipes de développement de Tiki Wiki et de Cypht, et s'enrichit à chaque version. C'est précisément ce qui distingue le logiciel libre, un outil qui

progresse, porté par plusieurs communautés qui convergent vers un même but, plutôt que de dépendre du bon vouloir d'un éditeur unique.

Concrètement, ce niveau avancé d'intégration permet par exemple de :

- Rechercher sur toutes vos boîtes à la fois, sans jongler entre onglets et applications.
- Transformer un email en donnée structurée. C'est la fonctionnalité qui change tout : un email peut devenir une fiche client dans votre suivi, une réclamation un ticket de support, un devis une pièce attachée au bon projet. L'email cesse d'être un flux incontrôlable pour devenir une information traçable et exploitable, stockée sur votre serveur et accessible à la seule équipe concernée.
- Migrer progressivement depuis Microsoft 365 / Google Workspace. Cypht est l'un des rares webmails open source à supporter Exchange Web Services en plus d'IMAP et SMTP. La bascule peut donc se faire en douceur, sans coupure, pendant que vos utilisateurs continuent de travailler.
- Automatiser le tri via des règles configurables (filtres Sieve) appliquées côté serveur, et intégrer calendrier et contacts (CalDAV, CardDAV).

Soyons clairs : ce niveau d'intégration demande une vraie réflexion sur vos processus, et ne s'improvise pas. C'est un projet en soi, que l'on étudie au cas par cas. Mais il illustre une chose essentielle : choisir l'open source, ce n'est pas se contenter d'un substitut au rabais. C'est parfois accéder à des possibilités que le logiciel propriétaire ne permet tout simplement pas.

## Changer d'outil sans paralyser vos équipes

La crainte est toujours la même : « si je change d'outil, je vais tout casser et paralyser mes équipes ». C'est légitime, et c'est précisément pour cela qu'une transition réussie ne se fait jamais d'un bloc.

Prenons un cas concret. Une petite structure veut quitter une messagerie américaine.
On ne bascule pas tout un lundi matin. On commence par le geste invisible pour les utilisateurs : sécuriser le nom de domaine et préparer le nouveau serveur en arrière-plan avec un hébergement souverain. Personne ne s'en aperçoit. Puis on déploie la nouvelle messagerie sur un premier poste, souvent celui d'une personne ou d'un groupe à l'aise avec l'informatique, qui devient le relais pour les autres. Une fois ce pilote concluant, on étend à une équipe, puis à une autre. Chacun avance au rythme où il s'approprie l'outil. Les deux environnements coexistent le temps nécessaire, sans coupure. Et un jour, sans heurt, la bascule est complète : tout le monde est passé, sans avoir eu l'impression de vivre une révolution.

C'est la force d'une migration étagée. Elle s'appuie sur des relais internes, respecte le rythme de chacun, et transforme un chantier intimidant en une suite de petits pas maîtrisés. C'est aussi là que notre accompagnement et la formation de vos équipes font la différence : un outil souverain bien adopté vaut mille fois mieux qu'un outil imposé.

## La visioconférence : le changement le plus simple

Une réunion stratégique, un entretien confidentiel, la présentation d'un dossier client : ces échanges ne devraient transiter par aucun serveur que vous ne maîtrisez pas. Pourtant, chaque appel Zoom ou Teams fait passer vos conversations, et souvent leurs transcriptions, par une infrastructure américaine. Cette défiance n'a rien de marginal : l'État français lui-même a décidé de bannir Teams, Zoom et Google Meet de ses services pour leur substituer sa propre solution de visioconférence sécurisée 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 open source à Teams et Zoom tient la route à grande échelle.

Le plus troublant n'est pas ce que ces plateformes avouent, mais ce qu'elles se gardent de promettre : aucune n'écrit noir sur blanc la seule phrase qui vous rassurerait vraiment, « rien n'est transcrit, rien n'est conservé, tout est détruit à la fin de la réunion ». On vous explique plutôt qu'on n'exploitera pas vos échanges « sans votre consentement », formule qui, en creux, reconnaît que la donnée est captée et qu'il ne manque qu'une case à cocher, que l'organisateur peut d'ailleurs cocher pour tout le monde. Pour faire simple il faut garder ce principe en tête : ce qui passe sur le réseau public ne vous appartient plus, et quelqu'un s'en sert déjà. Nous y reviendrons dans un prochain article consacré à ces conditions d'utilisation hallucinantes.

### Jitsi Meet : la visio souveraine, sans friction

Le mal est donc le même que pour l'email, mais le remède, ici, est d'une simplicité déconcertante. C'est même probablement la migration la plus indolore de toute la démarche : vos utilisateurs ne verront quasiment pas la différence, aucune résistance à prévoir. Jitsi Meet remplace Zoom et Teams pour les réunions vidéo : open source, chiffré, utilisable sans compte ni installation. Attention, cela ne veut pas dire "service minimum" pour autant : gestion des permissions d'accès, salles protégées par mot de passe, invitations contrôlées, modération des participants, tout est là pour garder la maîtrise de qui entre et de ce qui s'y dit.

Un simple lien dans le navigateur suffit, l'expérience est optimisée à l'extrême. Vous pouvez utiliser un hébergement souverain et installer Jitsi sur un serveur interne ou vous appuyer sur une instance européenne souveraine, et la qualité reste comparable aux solutions propriétaires pour

des réunions jusqu'à trente ou cinquante participants. Vous y retrouvez toutes les fonctions attendues : mode présentateur, partage d'écran, chat intégré, lever de main, arrière-plans floutés, enregistrement des sessions et diffusion en direct si besoin. Rien ne manque à l'appel pour mettre en place une alternative open source à Teams et Zoom.

### BigBlueButton : quand vous avez besoin de plus

Pour les structures aux besoins plus poussés, BigBlueButton, conçu à l'origine pour l'enseignement, va encore plus loin : tableau blanc partagé et annotation collaborative, salles de sous-commission, sondages en direct, partage de documents et enregistrement complet des sessions. Cette richesse a une contrepartie : BigBlueButton est plus gourmand en ressources serveur que Jitsi. C'est un arbitrage à poser selon vos usages réels, et c'est précisément le genre de choix que nous vous aidons à trancher.

Là encore, aucune donnée ne devrait transiter, par des serveurs américains. Aucun compte Microsoft ou Google n'est requis, et vos interlocuteurs externes vous rejoignent en un clic, sans rien installer. C'est l'exemple parfait du faux dilemme que l'on vous vend trop souvent : non, reprendre le contrôle ne signifie pas renoncer au confort. Ici, vous gagnez sur les deux tableaux.

## Le maillon faible, c'est presque toujours l'humain

On peut sécuriser ses serveurs, chiffrer ses communications, héberger ses données en Europe : il restera toujours une faille que la technique seule ne couvre jamais, le comportement humain. La sécurité ne devrait jamais reposer sur la vigilance d'une seule personne, et pourtant c'est souvent là que tout se joue. Nous l'avons illustré ailleurs avec l'histoire de la clé USB « oubliée » et de l'affaire Stuxnet : le maillon faible n'est presque jamais le système.

Et ce maillon, pour une organisation, c'est très souvent sa messagerie professionnelle. L'email reste le premier vecteur de la grande majorité des cyberattaques, et près de neuf entreprises françaises sur dix déclarent avoir subi au moins une tentative de phishing dans l'année. Le scénario est devenu un classique : un email qui imite à la perfection un dirigeant, un fournisseur ou un avocat, envoyé au bon moment, une veille de congés ou une clôture comptable, et qui réclame un virement urgent ou un changement de coordonnées bancaires. Pas de virus, pas de pièce jointe suspecte : juste de la manipulation. Et lorsqu'une boîte professionnelle est compromise, elle devient une clé maîtresse qui permet de réinitialiser les autres comptes, d'intercepter des codes et de surveiller vos échanges pour frapper au moment opportun.

C'est pourquoi reprendre le contrôle de sa communication ne s'arrête pas au choix des outils. Une messagerie souveraine bien configurée pose déjà les bonnes fondations : l'authentification du domaine par SPF, DKIM et DMARC complique l'usurpation de votre identité, et une supervision attentive repère les comportements anormaux. Mais la technique ne fait pas tout. Elle doit s'accompagner de réflexes simples chez vos équipes : se méfier de l'urgence, vérifier une demande inhabituelle par un autre canal, ne jamais réutiliser le mot de passe de sa boîte mail ailleurs, idéalement en s'appuyant sur un gestionnaire de mots de passe souverain, hébergé sous votre contrôle. C'est précisément là que la formation de vos collaborateurs fait la différence, et c'est un volet que nous intégrons à chaque déploiement.

## En résumé : par où commencer

Reprendre le contrôle de sa communication suit une logique simple, et c'est ce qui la rend accessible. Vous devez commencer par évaluer l'existant : quels services utilisez-vous, où sont hébergées vos données, qu'est-ce qui relève d'une juridiction étrangère, et qu'est-ce qui est réellement critique pour votre activité. De cette évaluation doit naître un plan, ordonné par priorité et par facilité de bascule.
Vous devez attaquer par le plus important et, justement, le moins complexe. D'abord le nom de domaine et les enregistrements DNS, le socle qui porte toute votre messagerie professionnelle. Ensuite le serveur d'emails et les clients, à déployer progressivement, équipe par équipe, sans coupure. Puis la visioconférence sécurisée, alternative open source à Teams et Zoom, la migration la plus indolore de toutes. Et enfin la consolidation des accès, pour ne pas laisser le facteur humain défaire ce que la technique a sécurisé.

Chaque étape doit être autonome, réversible, et apporter un gain immédiat : vous devez avancer à votre rythme, sans jamais tout remettre en jeu d'un coup.

Vous vous demandez par quelle brique commencer, et vous préférez garder vos ressources internes concentrées sur votre cœur de métier ? Ne perdez ni temps ni énergie : faites-vous accompagner et contactez nos experts. Choisir l'open source, c'est aussi soutenir un écosystème ouvert et des compétences proches de vous, plutôt que d'alimenter la rente d'un géant lointain. Ce type de mise en place est aujourd’hui courant dans les PME souhaitant reprendre le contrôle de leurs outils.

Le premier pas est souvent plus simple qu'on ne le croit, et le prochain volet de cette série sera consacré à la sécurisation de vos accès.