Protéger le Patrimoine Digital :
Un Enjeu Capital pour les Gouvernements & Les Administrations Publiques

Les Cyberattaques ciblant les Gouvernements et les Administrations Publiques ont atteint des niveaux inégalés, qu'elles émanent directement d'Etats étrangers ou de Groupes Privés de Cybercriminels.

Le niveau de Confidentialité des Informations qu'elles échangent, combiné avec leur périmètre d'intervention de plus en plus large, implique plus que jamais une réflexion critique sur la Sécurité de leurs communications distancielles.

Ce dossier présente une Synthèse des meilleures pratiques observées dans l'utilisation de Plateformes Sécurisées de Communication et de Collaboration dans la Sphère Publique.

Le Coût Global du CyberCrime dans les secteurs privés et publics.

$6'000 Mds par an

*projections d'Accenture pour 2021

113 Administrations Publiques

victimes de demande de Cyber Rançons en 2019, dont 90% ont été finalement payées.

Evaluation des Risques / 2020*

Pays	Risque n°1	Risque n°2	Risque n°3	Risque n°4
Royaume Uni	Cyberattaques	Crises Fiscales	Catastrophes Naturelles	Propagation de Maladies Infectieuses
Allemagne	Cyberattaques	Migrations de Population	Bulles d'Actifs Financiers	Propagation de Maladies Infectieuses
Pays Bas	Cyberattaques	Propagation de Maladies Infectieuses	Echec des Politiques « Climat »	Bulles d'Actifs Financiers
Etats Unis	Cyberattaques	Propagation de Maladies Infectieuses	Fraudes & Vols de Données	Catastrophes Naturelles
France	Instabilité Sociale	Propagation de Maladies Infectieuses	Chômage & Sous Emploi	Cyberattaques

*Données fournies par le World Economic Forum / Etude 2020 identifiant les préoccupations des acteurs économiques pour la prochaine décennie.

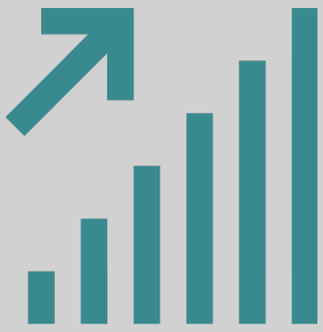
Selon le dernier rapport « Risks For Doing Business 2020 » du Forum Economique Mondial (World Economic Forum), le Risque lié aux Cyberattaques se positionne en moyenne au troisième rang du classement des préoccupations des acteurs économiques, après ceux liés au Chômage et aux effets des Crises Sanitaires.

Dans certains pays comme le Royaume Uni, l'Allemagne, les Pays Bas et les Etats Unis, il est même la principale préoccupation citée. **Plus que jamais, les entreprises privées et publiques sont dans l'obligation de re-prioriser et repenser leur stratégie de protection de leurs actifs numériques**.

Les 5 Principes pour sécuriser son Infrastructure de Communication

Le fondement d'une Architecture axée sur la Sécurité, repose sur l'utilisation de protocoles de communication de Dernière Génération. Chaque échange doit être systématiquement analysé et authentifié c'est l'approche « Confiance Zéro » (Zero Trust).

Ainsi chaque communication digitale au sein d'une Agence Gouvernementale ou d'une Administration Publique, s'effectue avec le même niveau de Sécurité et de Confidentialité q'un échange présentiel dans un cadre physiquement sécurisé.



La crise sanitaire actuelle voit une recrudescence massive du nombre de cyberattaques, notamment par le biais d'Usurpation d'Idendité d'Administrations Publiques Notoires. **Les analystes du FBI s'accordent à dire qu'elles auraient augmenté globalement de plus de 400%, depuis le début de la pandémie du Covid-19.**

1. Cryptage de Pointe

Le Cryptage de Bout en Bout (End to End Encryption ou E2EE) est devenu une nécessité incontournable, pierre angulaire de la Sécurité des Communications Digitales. Cependant de grandes disparités existent.

Le Principe de Confidentialité Persistante (Forward and Backward Secrecy) est en effet le seul à garantir le cryptage unique de chaque échange, à la différence d'une clé protégeant globalement l'ensemble du Sytème de communication. De même, l'efficacité des différents protocoles de cryptage demeure très inégale. **Seul un protocole basé sur le double cryptage de bout en bout (double ratchet)** permet effectivement une protection individuelle de chaque appel, visioconférence ou message et ce en fonction de l'appareil utilisé : **c'est le principe même de la « Doublé Clé de Protection »**.

Chacune d'entre elle est générée de manière unique, et non plus par un serveur hébergé dans une Infrastructure plus ou moins proche. **La protection des échanges est donc assurée jusqu'au plus petit dénominateur de l'Infrastructure (l'ordinateur, le téléphone ou la tablette)** ce qui réduit considérablement les chances d'être victime d'une Cyberattaque.

2. Souveraineté des Données

La « Donnée » est devenue pour tous les secteurs d'activité un enjeu crucial. Il l'est encore plus pour les Gouvernements et les Administrations Publiques, compte tenu de leur mission et de la complexité des Cybermenaces.

Elles doivent donc prioriser la Souveraineté de leurs Données en implémentant des Politiques Techniques basées sur la « **Confiance Zéro** » **(« Zero Trust »)** et héberger leurs données dans des Infrastructures de Cloud Privé ou d'Environnements Propres (On Premises).

3. Continuité de Service

Un enjeu crucial (et souvent négligé), est la capacité d'assurer la continuité des services de Communication lorsque l'Infrastructure est compromise par une Cyberattaque.

Si un Gouvernement ou une Administration Publique ne sont pas mesure de fournir **une Solution de Gestion de Crise autonome et indépendante de leur Infrastructure**, leurs agents, pour continuer à collaborer, trouveront « trop » rapidement des solutions alternatives de communication bien moins sécurisées et beaucoup plus risquées.

De facto, les données confidentielles et sensibles apparaîtront avec beaucoup plus de probabilité sur les écrans Radar des Cybercriminels - exposant aussi l'Organisation à un risque accru de non respect des Règles de Confidentialité des données (RGPD).

4. Fédération & Standard « Messaging Layer Security »

Wire™ dirige actuellement le développement du nouveau standard Open Source de communication sécurisée « **Messaging Layer Security (MLS) », ** au sein de l'Internat Engineering Task Force (IETF).

En partenariat avec les acteurs majeurs de l'Industrie, notre objectif est de créer la prochaine génération d'un système fédéré et interopérable. I**l doit permettre de communiquer via différentes plateformes tout en garantissant le même niveau de Confidentialité et de Sécurité que celui proposé nativement par Wire.** Le co-fondateur et ancien dirigeant de Skype, Alan Duric, pilote cette initiative (après avoir notamment élaboré le standard WebRTC), qui a pour objectif de créer la prochaine génération de protocole de cryptage.

La fonctionnalité de Fédération permet à plusieurs entités d'une même Administration Publique, de communiquer entre elles sur leur Intranet, tout en sécurisant leurs communications.

5. « Hyper Transparence »

Les stratégies de protection des actifs numériques, doivent allier Sécurité, Confidentialité et Transparence, lorsqu'il s'agit de communiquer sur des plateformes sécurisées. Et le meilleur moyen est d'y parvenir est d'utiliser une solution dont le **code est OpenSource.**

Il est en effet bien moins opaque dans sa construction et son fonctionnement. Il garantit que son éditeur est profondément attaché aux notions de partage de son architecture native de Sécurité - et qu'il peut être évalué et audit par des organismes de certification indépendants -

L'accès au code Open Source permet donc d'identifier précisément les choix effectués par l'éditeur d'une solution, dans le traitement des données, les modèles d'intégration, le stockage des clés de cryptage et tout autre source potentielle de risque Cyber.

Sélectionner une Solution de Collaboration & de Communication

Le marché actuel proposant un grand choix de solutions, le choix peut sembler difficile.

Nous encourageons les Gouvernements et Administrations Publiques à consulter ces recommandations pour minimiser leur exposition aux Attaques Cybercriminelles.

Tableau Comparatif*

*Tableau comparatif issue de l'Etude CyberSécurité de la NSA «Comment Sélectionner et Utiliser en toute sécurité une Solution de Télétravail»

	E2EE Text Chat	E2EE Voice Calls	E2EE Video Calls	E2EE File Sharing	E2EE Screen Sharing	Open-source Code	Certified Service
Wire	✓	✓	✓	✓	✓	✓	FedRAMP In Progress
Cisco Webex	✓	✓	✓	✓	✓	X	FedRAMP
Dust	✓	N/A	N/A	N/A	N/A	X	None
Google G Suite	X	X	X	X	X	X	FedRAMP
GoToMeeting	✓	✓	✓	N/A	N/A	X	None
Jitsi Meet	✓	✓	✓	✓	✓	✓	None
Mattermost	X	X	X	N/A	X	✓	None
Microsoft Teams	X	X	X	X	X	X	FedRAMP
Signal	✓	✓	N/A	✓	N/A	✓	None
Skype for Business	X	X	X	X	X	X	FedRAMP
Slack	X	X	X	X	X	X	FedRAMP
WhatsApp	✓	N/A	✓	✓	N/A	X	None
Wickr	✓	✓	✓	✓	✓	✓	None
Zoom	✓	X	X	✓	X	X	FedRAMP

Légende: N/A = Non Applicable

Pourquoi Wire?

Les Gouvernements et Administrations Publiques, qui ont choisi Wire, souhaitent évidemment contrôler au mieux leurs informations sensibles tout en offrant à leurs agents une plateforme de communication Conviviale et Sécurisée.

Que ce soit en télétravail ou en déplacement, leurs utilisateurs peuvent instantanément passer un appel audio, organiser une visioconférence, envoyer des messages et partager leurs fichiers, sans mettre en danger l'intégrité de leurs données.

Conçu pour fonctionner dans les Environnement Classifiés



INSTALLATION ON-PREMISE (Online & Offline)

ACCREDITATION BSI (Bundesamt für Sicherheit in der Informationstechnik)

FEDERATION

AUDITS EXTERNES

CODE 100% OPEN SOURCE

CONFORMITE RGPD

Wire et son approche «Security by Design» sont reconnues comme Leader par la société de conseil et d'évaluation International Data Corporation (IDC).

Le Cas d'Usage du Gouvernement Allemand

Avec un nombre croissant d'agents contraints au télétravail compte tenu de la crise sanitaire actuelle, la protection des communications sensibles à distance, est devenue plus que critique.

Le Gouvernement Allemand a choisi Wire, pour s'adapter rapidement à ses nouveaux modes de travail tout en réduisant drastiquement ses risques de Sécurité. L'Office Fédéral de la Sécurité des Technologies de l'Information (*Bundesamt für Sicherheit in der Informationstechnik* or *BSI*) recommande en effet Wire comme l'outil officiel de Communication Sécurisée pour l'échange d'Informations Classifiées.

L'ensemble de nos fonctionnalités - message, appel audio, visioconférence et partage de fichiers - couplé à une interface ergonomique font de Wire une solution moderne et intuitive très appréciée par ses utilisateurs.

Une Sécurité Inégalée

- Recommandé par la NSA & le BSI
- Principe de « Confidentialité Persistante »
- Conforme Mission Publique
- Empreinte minimal en terme de métadonnées
- Développé par les anciens ingénieurs de Skype

Richesse des Fonctionnalités

- Suite Complète de Collaboration
- Configuration du Mode Ephémère
- Salons d’Invité Externes Sécurisés
- 12 Participants en Visioconférence
- 25 Participants en Appel Audio
- Fonctionne en faible bande passante

Convivialité

Bénéficiant d’un design épuré et d’une interface intuitive que nos utilisateurs plébiscitent, Wire est une application facile à utiliser. Elle est disponible sur iOS, Android, Windows, Mac, et Web App jusqu’à 8 appareils par utilisateur.

Cas d’Usage pour les Gouvernements et Administrations Publiques



Protection des Informations Critiques



Protection face au Cyber-Espionnage



Sécurité des Communication Mobiles



Réponse Immédiate aux Incidents

Wire Entreprise

Plateforme entièrement personnalisable, hébergée dans votre Infrastructure et selon vos paramètres, pour garantir la Sécurité de vos Echanges Collaboratifs, en conformité avec les standards du marché les plus exigeants.

CONTACT US ▶

Wire Pro

Plateforme en mode à la demande (Software as A Service) chiffrée de bout en bout. Créez votre compte, invitez vos collègues et vous pouvez immédiatement communiquer et collaborer avec le plus haut niveau de Sécurité.

GET STARTED ▶



> Wire a été un choix évident pour Fortum - leur plateforme de Collaboration est non seulement hautement sécurisée grâce à son protocole de cryptage, mais ils l'ont construite selon des principes de transparence et de confidentialité uniques, que beaucoup d'autres solutions du marché n'ont pas.
> **Tomas Nystrom, Directeur des Systèmes d'information Fortum.**

Wire™ en deux mots

Wire™ est la plateforme de collaboration la plus sécurisée du marché, transformant les modes de travail au sein des organisations privées et publiques, au même rythme que ces fondateurs ont révolutionné le monde de la Téléphonie il y a quelques années, en créant Skype.

Basée à Berlin avec des bureaux en Suisse et à San Francisco, Wire, plusieurs fois primée, compte plus de 1 800 clients dans le Monde. Reconnue par les grands cabinets de conseil comme IDC, Forrester, et Gartner, Wire propose une solution complète de messagerie, de visioconférence, d'appel, de partage de fichier et de collaboration avec vos clients, partenaires et prestataires externes - chacune de ces interactions étant protégées par le protocole de cryptage de bout en bout le plus élaboré du marché.

Visitez notre site wire.com pour découvrir nos solutions adaptées aux cas d'usage des Agences Gouvernementales, Militaires et des Administrations Publiques.

Récompenses

INFOSEC AWARDS WINNERS CYBER DEFENSE MAGAZINE 2020

Capterra BEST EASE OF USE 2019

Leader FALL 2020

Capterra TOP 20 2020

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

La confiance de nos Partenaires

INTELLIGENT WAVES LLC

DELL Technologies

BYLIGHT

SVA