CALIALABS

CEREBRO INTELLIGENCE SERIES

RPT-2025-01

Novembre 2025

PUBLIC / STRATÉGIQUE

/// COMPLIANCE

L'ANGLE MORT DE L'ARTICLE 30 DORA : LE RISQUE SMTP SORTANT

Analyse d'écart critique entre les exigences de résilience opérationnelle (DORA) et les infrastructures de messagerie cloud natives.

SYNTHÈSE EXÉCUTIVE

Le Règlement (UE) 2022/2554 (DORA), entré en pleine application le 17 janvier 2025, impose aux entités financières une maîtrise absolue de leurs risques TIC. L'Article 30, en particulier, redéfinit la responsabilité de l'institution vis-à-vis de ses prestataires tiers.

Pourtant, les audits récents révèlent une faille systémique dans la majorité des Fintechs européennes : **les communications emails sortantes**. Transitants par des infrastructures Cloud (Microsoft 365, Google Workspace), ces flux échappent aux contrôles granulaires de conformité, constituant le vecteur de risque n°1 non surveillé.

2. ANALYSE JURIDIQUE : L'IMPASSE DE L'ARTICLE 30

La réglementation DORA ne se contente pas d'exiger la sécurité ; elle exige la **preuve de la maîtrise**.

2.1. La Responsabilité Primaire (Art. 30)

Contrairement aux idées reçues, l'externalisation de la messagerie vers un géant du Cloud (Microsoft/Google) ne transfère pas la responsabilité réglementaire.

> **Citation DORA :** "En cas de manquement d'un prestataire tiers, l'entité financière conserve l'entière responsabilité du respect de ses obligations au titre du présent règlement." (Considérant 76)

2.2. L'Exigence d'Intégrité (Art. 30-2-d)

Les accords contractuels doivent garantir l'accessibilité, la disponibilité, l'intégrité et la sécurité des données. Or, un email envoyé par erreur à un destinataire externe via une infrastructure standard viole le principe de confidentialité dès sa sortie du serveur.

> ⚠ **L'Échelle des Sanctions**
>
> - **Défaut de notification (24h)** : Violation DORA Art 19.
> - **Violation de données personnelles** : Jusqu'à 4% du CA mondial (RGPD).
> - **Impact ACPR** : Risque de blâme ou de retrait d'agrément pour défaut de contrôle interne.

3. LE CONSTAT D'ÉCHEC DES DLP "LEGACY"

L'industrie financière s'appuie encore majoritairement sur des DLP (Data Loss Prevention) statiques. Notre analyse technique démontre leur incapacité structurelle à stopper les fuites modernes.

3.1. La Cécité Contextuelle (L'échec du Regex)

Les DLP traditionnels scannent des motifs (ex: `[0-9]{16}` pour une carte de crédit).

- → **Le Problème** : Si un collaborateur envoie un fichier client "nettoyé" (sans numéros de CB) mais contenant des données stratégiques ou des informations KYC sensibles, le DLP reste muet.
- → **La Réalité** : Un moteur basé sur des règles ne comprend pas l'intention. Il ne peut pas distinguer une erreur légitime d'une exfiltration malveillante reformulée.

3.2. La Fatigue des Alertes

400h	85%	0%
PERDUES PAR AN / ÉQUIPE	FAUX POSITIFS DLP	COMPRÉHENSION DU CONTEXTE

4. AUTOPSIE D'UN INCIDENT : LA FINTECH "X"

Étude de cas anonymisée d'une Scale-up de paiement française (Série B).

LE SCÉNARIO

Un vendredi à 17h45, le Responsable Conformité souhaite envoyer un export de la base "Clients à Haut Risque" (KYC) à son adjoint. Par erreur d'autocomplétion dans Outlook, il sélectionne un homonyme externe (un journaliste).

- → **L'Échec du DLP** : Le fichier Excel ne contenait pas de numéros de carte bancaire. Le DLP Microsoft 365 n'a rien détecté. L'email est parti instantanément.
- → **L'Angle Mort** : L'incident n'a été découvert que 4 jours plus tard, suite à une réponse du destinataire.

⚠ Conséquence Réglementaire

- Dépassement du délai de notification DORA (24h).
- Violation de confidentialité RGPD.
- Audit d'urgence déclenché par l'ACPR.

Diagnostic : Ce n'est pas une erreur humaine, c'est une erreur d'architecture. Le système a autorisé l'envoi d'une donnée critique vers un domaine non-autorisé sans analyse sémantique préalable.

5. LA SOLUTION ARCHITECTURALE : COMPLIANCE-BY-DESIGN

Pour se conformer à l'état de l'art et aux exigences des RTS (Regulatory Technical Standards), l'architecture de messagerie doit évoluer vers un modèle d'**Interception Active**.

5.1. Le Modèle "Smart Host" (Server-to-Server)

- → **Passerelle SMTP Sécurisée**: Tous les emails sortants transitent par une instance d'analyse dédiée avant d'atteindre l'Internet public.
- → **Chiffrement Forcé**: TLS 1.3 imposé pour garantir l'intégrité du canal.

5.2. L'Intelligence Sémantique

L'analyse ne doit plus chercher des mots-clés, mais **comprendre des intentions**.

DÉTECTION VECTORIELLE

Le système doit comprendre que "Voici la liste des clients" envoyé à une adresse @gmail.com est une anomalie critique, quel que soit le contenu du fichier joint.

5.3. L'Auditabilité WORM

Chaque décision de blocage ou d'envoi doit être journalisée dans un format WORM (Write Once, Read Many), garantissant l'immutabilité de la preuve en cas d'investigation.

CONCLUSION

Le risque SMTP sortant n'est plus une hypothèse technique, c'est une responsabilité juridique. Dans l'ère post-DORA, l'ignorance de ce canal ne constitue plus une défense recevable. Les institutions financières doivent migrer d'une surveillance passive vers une **interception intelligente active** pour protéger leur licence.