



La migration, moment de vulnérabilité : les précautions cyber

Une migration télécom est une période particulière : des équipements neufs arrivent, des prestataires interviennent, des accès sont créés dans l'urgence pour « faire fonctionner », et l'on remet à plus tard ce qui n'empêche pas les appels de passer. C'est exactement la fenêtre pendant laquelle une installation devient vulnérable — et le « plus tard » n'arrive jamais. Voici les précautions à intégrer au chantier, avec un avertissement particulier sur le risque le plus coûteux : la fraude téléphonique.

Le risque n°1 : la fraude téléphonique

Commençons par celui qui coûte le plus cher et se manifeste le plus vite. Une installation téléphonique mal protégée peut être détournée pour générer des appels vers des destinations surtaxées, la nuit ou le week-end — avec une facture qui arrive ensuite, parfois très salée. C'est le sujet développé dans [sécuriser sa téléphonie IP contre la fraude](#). Les périodes de migration y exposent particulièrement, pour une raison simple : les protections sont souvent **désactivées** « **le temps des tests** » et réactivées plus tard — ou jamais. Trois parades élémentaires : des **mots de passe robustes** sur tous les comptes, une **restriction des destinations** autorisées, et un **plafond de dépense** avec alerte, que la plupart des opérateurs proposent gratuitement.

Les six précautions du chantier

- **Changer tous les mots de passe d'usine** — box, routeur, switch, postes, interface d'administration de la téléphonie. C'est la première chose que cherche un attaquant, et la plus fréquemment oubliée sur du matériel installé rapidement.
- **Recenser les accès distants créés** pendant le chantier : intégrateur, éditeur, mainteneur. Notez qui a accès à quoi, et prévoyez de **refermer** ce qui était temporaire.
- **Refermer les ouvertures de test.** Les accès ouverts « pour vérifier » doivent être listés le jour où on les ouvre, avec une date de fermeture — sinon ils deviennent permanents par oubli.

- **Séparer la voix du reste** du réseau : c'est un bénéfice de sécurité autant que de qualité, expliqué dans [VLAN voix et réseau local](#).
- **Vérifier ce que les prestataires emportent** : plans de numérotation, listes de contacts, enregistrements. Ces données relèvent souvent du [RGPD](#), et leur sort doit être contractualisé.
- **Documenter la configuration finale**. Une installation dont personne ne connaît les réglages ne peut être ni auditée ni restaurée après un incident.

Le point aveugle : les accès de télémaintenance

La migration fait basculer des accès qui étaient jusque-là **isolés** — un fournisseur se connectait à son équipement par une ligne dédiée, sans toucher à votre réseau — vers des accès qui passent désormais **par votre système d'information**. C'est le sujet décrit dans [industrie, automates et télémaintenance](#), et il vaut aussi pour un ascenseur, une alarme, une chaufferie ou un logiciel métier. Bien conçu — accès nominatif, tracé, limité à l'équipement concerné —, c'est une amélioration nette. Improvisé, c'est une porte ouverte. La règle : chaque accès distant doit avoir un **propriétaire identifié** et une **raison d'exister**.

Pour les organisations soumises à des obligations

Collectivités, opérateurs de services essentiels, entités concernées par la directive NIS2 : la migration est aussi un moment de **traçabilité**. Ce qui est fait doit être documenté — inventaire des équipements, accès accordés, mesures prises, tests réalisés. Non par formalisme, mais parce que c'est exactement ce qui sera demandé en cas d'incident ou de contrôle. Les exigences sont détaillées dans [NIS2 et résilience télécom](#). Bonne nouvelle : le travail d'inventaire imposé par la fin du cuivre produit déjà l'essentiel de cette documentation.

En synthèse

- Le risque le plus coûteux et le plus rapide est la **fraude téléphonique** : mots de passe, restrictions, plafond d'alerte.
- Les mots de passe d'usine et les **ouvertures de test** sont les deux failles typiques d'un chantier.
- Chaque accès distant doit avoir un **propriétaire et une raison d'exister**.
- Documentez la configuration finale : c'est ce qui permet d'auditer et de restaurer.

Cet article donne des repères généraux à visée d'information et ne constitue pas un audit de sécurité. Les organisations soumises à des obligations réglementaires doivent se référer au

cadre qui leur est applicable et s'appuyer sur des spécialistes.

Pour aller plus loin

- [Sécuriser sa téléphonie IP : fraude téléphonique et parades](#)
- [NIS2 et résilience télécom : quelles exigences ?](#)
- [Le SBC expliqué au décideur](#)
- [RGPD et téléphonie IP](#)

Un chantier à sécuriser avant la mise en service ?

AILERYS Conseil porte les exigences de sécurité au cahier des charges et vérifie ce qui a réellement été fait à la recette.

[Échanger avec un expert : https://finducuire.info/contact/](https://finducuire.info/contact/)

À lire aussi dans ce dossier

- [VLAN voix et alimentation par le câble](#)
- [Industrie : automates, GTC et télémaintenance](#)
- [Le plan de recette : vérifier que tout fonctionne](#)
- [Choisir son intégrateur télécom : les critères qui comptent](#)

Article révisé le 21 octobre 2026 par FinDuCuivre.info

<https://finducuire.info/migration-vulnerabilite-cyber-precautions/>