#NOM CLIENT#

#ADD 1#

#ADD 2#

#CP# #VILLE#

**A l’attention de #GENRE# #PRENOM# #NOM#**

Paris, le mardi 29 novembre y

Par LRAR

**Objet : Mise en œuvre de la sécurité de vos Autocommutateur PABX**

Madame, Monsieur, Cher client,

Toujours soucieux de votre sécurité, nous sommes amenés à vous rappeler que les risques d’attaques envers les autocommutateurs téléphoniques (PABX) reportés au CERT-FR\* sont de plus en plus nombreux.

Nous vous demandons donc de prêter une attention toute particulière à la sécurité́ de vos PABX, en appliquant, à minima, les mesures suivantes :

* Vérifier le contrat de maintenance ou d’externalisation de l’exploitation associés à votre équipement. Si aucune obligation de surveillance du système n’est prévue dans le contrat, souscrivez une prestation de surveillance du système par le prestataire (journaux, relevés d’incidents, etc.) avec protocoles de transmissions d’informations et d’alerte ainsi qu’une assurance contre la fraude téléphonique;
* Intégrer l’autocommutateur au référentiel de sécurité́, au même titre que les autres composants du système d’information ;
* Assurez-vous de bénéficier de la dernière mise à jour de votre PABX ;
* Qualifier puis appliquer les derniers correctifs de sécurité́ du constructeur ;
* Appliquer une politique de mots de passe forts qui devront être régulièrement changés pour l’administration de l’autocommutateur ;
* Vérifier la configuration adéquate des droits des utilisateurs, notamment pour l’autorisation d’appels à l’international, la consultation de la messagerie à distance et la fonction de rappel depuis la messagerie ;
* Initialiser les codes d’accès des postes téléphoniques et des boites vocales des utilisateurs à des valeurs autres que celles par défaut et non triviales (0000, 1234, etc.) ;
* Demander aux utilisateurs déjà̀ enregistrés d’adopter un code non trivial et de le changer régulièrement. Si l’autocommutateur dispose d’une fonctionnalité́ permettant d’empêcher la configuration de codes d’accès triviaux (0000, 1234, etc.) celle-ci doit être activée ;
* Désactiver la fonction DISA (*Direct Inward System Access* : fonctionnalité́ permettant à un utilisateur externe d’accéder aux fonctionnalités du commutateur normalement accessibles uniquement en interne) si elle n’est pas nécessaire ou, dans le cas contraire, limiter les services de l’autocommutateur accessibles via cette fonction et les personnes pouvant accéder à ce service.

Il est également vivement recommandé de rechercher la présence d’anomalies pouvant être le signe d’une compromission d’un autocommutateur. Ces anomalies peuvent être une facturation téléphonique d’un montant inhabituel ou des appels vers des destinations estrangères sans rapport avec l’activité́ professionnelle.

Nous vous proposons d’analyser à nouveau votre installation afin de la mettre en adéquation avec les règles de sécurités citées ci-dessus. L’objectif étant de minimiser les risques de fraude téléphonique.

Le risque de fraude téléphonique ne pouvant être réduit à néant et votre satisfaction étant notre principale préoccupation nous nous proposons une tarification particulière pour cet audit.

Dans l’attente de vous rencontrer, nous vous prions d’agréer, Cher Client, l’assurance de nos sentiments distingués.

La Direction

*(\*): Le CERT-FR, le centre gouvernemental de veille, d’alerte et de réponse aux attaques informatiques,* [*http://cert.ssi.gouv.fr*](http://cert.ssi.gouv.fr)*, est une des composantes curatives complémentaires de l’ANSSI (Agence Nationale de Sécurité des Systèmes d’Information).*