FIBRE OPTIQUE

Des opérateurs alternatifs interpellent l'Arcep

Dans une lettre à destination de l'Arcep, Nerim, Sewan et Alphalink veulent démontrer au régulateur l'important que peuvent jouer les opérateurs alternatifs sur le marché des offres de très haut débit à destination des entreprises.

Lancée par l'Arcep (le régulateur des télécommunications) au mois de juin dernier concernant, notamment, le raccordement des entreprises à la fibre optique, n'a pas manqué de faire réagir les opérateurs de services à destination des entreprises. Alexandre Nicaise, Bernard Lemoine et David Brette, respectivement dirigeants d'Alphalink, Nerim et de Sewan, ont, dans une missive adressée au régulateur, rappelé le rôle que peuvent jouer les opérateurs alternatifs dans le développement de services Très Haut Débit à destination des entreprises.

Pour le trio, l'Arcep ne prend pas en compte la totalité des acteurs du marché dans sa réflexion. « *Vous segmentez le marché depuis les gros acteurs du segment [que sont Orange et SFR (propriété d'Altice, comme le Journal des télécoms, ndlr)] jusqu'aux opérateurs de proximité. Vous expliquez que ces derniers n'investissent pas* », regrette le trio. Les trois opérateurs estiment, au contraire avoir investi, indirectement en exploitant les réseaux développés par des opérateurs tiers grâce à « *l'apport d'un nombre significatif de clients* ».

OFFRES DE RÉFÉRENCE DE GROS

Alphalink, Sewan et Nerim pointent dans leur courrier, une situation concurrentielle qui les désavantage. Pour eux, l'impossibilité de proposer leurs services dans les zones denses ou les zones AMII (zones dans lesquels les opérateurs publics et privés ne peuvent se concurrencer) constituent un frein au développement de leurs activités d'une part, et au développement des services fibre à destination des entreprises. L'ouverture des réseaux fibre dans ces zones leur permettrait de proposer leurs services plus aisément aux entreprises. En outre, le trio demande des offres de référence de gros sur les réseaux fibre « *comme il en existe sur le cuivre* », précisent les auteurs du courrier.

Cette lettre intervient dans un contexte bien particulier. L'extinction programmée du réseau commuté d'Orange, utilisée par les entreprises et les opérateurs, pousse les utilisateurs de ce réseau à se tourner vers d'autres solutions comme la fibre optique.

THOMAS PAGBE

SÉCURITÉ

L'authentification forte proposée par Transatel

Comment se prémunir contre les faiblesses des systèmes d'authentification ? Un SMS chiffré de bout en bout redonne de la sérénité aux DSI et RSSI.

Les cadres en situation de mobilité ont aujourd'hui besoin de pouvoir se connecter à tout moment aux serveurs de l'entreprise. Or, si la connexion vers ces serveurs est souvent sécurisée par des logiciels dédiés, **le maillon faible demeure l'authentification de l'utilisateur.**

L'authentification est pourtant cruciale pour s'assurer que la personne qui souhaite accéder aux ressources et applications critiques de l'entreprise est bien celle qu'elle prétend être. Il s'agit par exemple d'empêcher qu'un usurpateur puisse accéder aux serveurs de production.

Le principe du login/mot de passe, bien qu'encore largement utilisé dans les VPN par exemple, est notoirement insuffisant. Cela explique

l'apparition de solutions d'authentification fortes s'appuyant sur le téléphone portable comme deuxième facteur d'authentification.

Le principe des codes à usage unique reçus par SMS est aujourd'hui bien connu. Mais ce mécanisme protège-t-il réellement ?

Les rapports récents du NIST* et de l'Université d'Amsterdam** affirment le contraire : les SMS circulent en clair sur le réseau SS7 de signalisation des opérateurs et peuvent donc être interceptés par des tiers malveillants.

Ils sont aussi de plus en plus vulnérables sur les smartphones, à cause de virus (sur Android) ou des mécanismes de synchronisation (sur iOS). Transatel a trouvé la parade : utiliser la carte SIM pour sécuriser ces SMS.

Grâce à la solution de Transatel, le SMS est chiffré de bout en bout entre le serveur d'authentification et la carte SIM.

La saisie d'un code PIN dédié est obligatoire pour décoder le contenu du SMS. L'authentification forte de l'utilisateur devient ainsi réellement efficace.

Et le grand avantage de la solution est qu'elle ne change rien aux habitudes : qui n'a pas déjà confirmé un achat sur Internet via un code reçu par SMS ?

* *Digital Authentication Guideline, National Institute of Standards and Technology (NIST), 2016*

** *How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication, Radhesh Krishnan Konoth, Victor van der Veen, and Herbert Bos, 2016*

Pour plus d'informations
info-security@transatel.com

www.transatel.com

transatel

PUBLI-RÉDACTIONNEL