



Berne,

13.01.2015

Désactivation du protocole de cryptage SSL v3

Faible de sécurité „Poodle“

Chères clientes, chers clients,

La faille de sécurité „POODLE“ permet d’intercepter les données sur une connexion cryptée avec le SSL v3.

C’est pourquoi, début mai, seules les communications cryptées avec TLS 1.0 ou supérieure seront acceptées.

Si, actuellement vous transmettez encore des messages à e-dec avec SSL v3, vous devez au plus tard pour le 28.04.2015 passer de SSL v3 à TLS 1.0 ou supérieure.

Afin que vous puissiez tester la configuration de votre système, nous allons publier une adresse URL-Test temporaire pour e-dec test. Dès que celle-ci sera disponible, nous vous en informerons.

En cas de doutes ou problèmes, les clients finaux comme p.ex. les maisons d’expédition, les transitaires, etc., sont priés de s’adresser à leurs prestataires de services informatiques ou leurs fournisseurs de logiciel.

Avec nos meilleures salutations

La permanence CSC