

21/01/2014

EPROTBC/2014
www.enisa.europa.eu

L'Agence européenne de cyber-sécurité ENISA plaide pour des services bancaires en ligne et des paiements électroniques sécurisés : il faut des identifiants non reproductibles et non réutilisables pour les documents d'identité numérique dans le secteur financier

Divers types de jetons, de dispositifs, de téléphones mobiles, de signatures électroniques, etc. sont utilisés pour authentifier notre identité numérique. Pourtant, selon une nouvelle étude effectuée par l'Agence de cyber-sécurité européenne ENISA, certaines institutions financières ne tiennent toujours pas compte des risques liés aux mécanismes d'authentification inappropriés. Le rapport analyse les fraudes courantes dans les services financiers électroniques «e-Finance» en les reliant aux mécanismes d'authentification «client» des institutions financières. Le rapport met l'accent sur la nécessité d'actualiser les mécanismes de sécurité et recommande dix approches pour une meilleure sécurité des services bancaires électroniques.

L'Agence a analysé plus d'une centaine de réponses à un sondage adressé aux banquiers et aux professionnels de la sécurité des services bancaires électroniques relatif aux méthodes d'authentification et d'identification électronique (eIDA), utilisées quotidiennement par les citoyens, les clients et les entreprises dans le secteur financier et les paiements bancaires électroniques. L'Agence a en outre identifié les risques et les types d'attaques de chaque mécanisme d'authentification, notamment l'hameçonnage (les attaques ciblées), le vol d'identité (ID-theft), l'usurpation d'identité et de session etc., des institutions financières, des banquiers et fournisseurs de services de transactions financières.

L'Agence a par conséquent élaboré des directives, et proposé de meilleures pratiques et recommandations relatives aux services bancaires et aux paiements électroniques. Elle recommande entre autres de :

1. Améliorer la sécurité dans le secteur du service bancaire électronique. Les acteurs du secteur financier devraient dans ce cas :

- Analyser les risques encourus en fonction du profil de chaque client et de la taille de l'institution ;
 - Sensibiliser davantage les clients et améliorer leurs compétences;
 - Concevoir des méthodes spécifiques d'authentification basées sur les comportements du client et les paramètres de ses transactions (ex. le pays destinataire, le montant de la transaction)
 - Détecter rapidement tout instrument utilisé par les clients et qui serait compromis lors de son enregistrement, tester et vérifier sa fiabilité. ("[Tout instrument est présumé infecté](#)")
- **2. Renforcer la sécurité des applications de services financiers électroniques et leurs canaux de distribution aux consommateurs** : encourager le concept habituel de " security by design". Il serait également souhaitable de tenir compte de la proposition pour la nouvelle [Directive de protection des données personnelles](#), et d'utiliser des canaux fiables pour installer les applications sur les appareils électroniques des clients.

L'ENISA est un centre d'expertise pour la sécurité des réseaux et de l'information en Europe

Sécuriser la société de l'information de l'Europe

L'Agence de l'UE pour la sécurité des réseaux et de l'information

21/01/2014

EPROTBC/2014
www.enisa.europa.eu

- **3. Promouvoir la proportionnalité entre l'efficacité de certaines méthodes proposées et les risques identifiés** (adéquation de l'eIDA en fonction du contexte de la transaction) en mettant l'accent sur l'usage de deux éléments d'authentification, même pour les opérations les moins risquées (ex. Les ATM possèdent : une carte et un code PIN)
- **4. Améliorer la connaissance et les habitudes bancaires des clients et des professionnels :**
En définitive, les pratiques actuelles de l'eIDA dans le secteur financier ne protègent pas des risques. L'ECB et la Commission européenne élaborent actuellement des recommandations qui tiennent compte du rapport de l'ENISA afin d'identifier et d'élaborer des instruments de réduction des pertes financières dues aux fraudes.

Le Professeur Udo Helmbrecht, [Directeur exécutif](#) de l'ENISA observe que: "Le secteur financier gère chaque année des transactions électroniques de plusieurs milliards d'euro. Les identités numériques sécurisées et leur authentification sont tout simplement une nécessité incontournable pour l'économie européenne. Les institutions financières devraient considérer la sécurité comme un instrument concurrentiel de marketing. Ce rapport devrait permettre aux acteurs du secteur financier d'analyser le ratio coûts/bénéfice apporté par les mécanismes d'authentification additionnels"

[Pour accéder au rapport complet :](#)

Contexte :

Les [recommandations de l'UE pour la directive de protection des données](#), et la [Directive 2 des Services de paiement](#), [ECB 2 «Recommandations pour la sécurité des paiements en ligne»](#)

Pour toute demande d'interviews, veuillez contacter : Ulf Bergström, Porte – parole
ulf.bergstrom@enisa.europa.eu, portable: + 30 6948 460 143, Manel Medina, ENISA Expert,
sta@enisa.europa.eu

Veuillez noter: traduction. La version anglaise est la seule version officielle

www.enisa.europa.eu/media/enisa-en-francais/

www.enisa.europa.eu

L'ENISA est un centre d'expertise pour la sécurité des réseaux et de l'information en Europe

Sécuriser la société de l'information de l'Europe

L'Agence de l'UE pour la sécurité des réseaux et de l'information