Sécuriser les données personnelles : Les directives de l'ENISA relatives aux solutions cryptographiques

L'ENISA lance aujourd'hui deux rapports. Le rapport de 2014 « Algorithmes, taille clé et paramètres » est le document de référence fournissant un ensemble de directives aux preneurs de décisions, en particulier, les spécialistes qui conçoivent et mettent en œuvre les solutions cryptographiques pour la protection des données personnelles au sein des organisations commerciales ou des services gouvernementaux pour les citoyens. L' « étude sur les protocoles cryptographiques » fournit une perspective de mise en œuvre, en couvrant les directives relatives aux protocoles exigées pour protéger les communications commerciales en ligne contenant des données personnelles.

« Algorithmes, taille clé et paramètres »

Ce rapport est un ensemble de propositions sous une forme facile à utiliser, mettant l'accent sur les services commerciaux en ligne qui recueillent, conservent et traitent les données personnelles des citoyens de l'Union européenne. Il fournit une mise à jour du rapport 2013, sur les directives cryptographiques relatives aux mesures de sécurité exigées pour protéger les données personnelles dans les systèmes en ligne. Par rapport à l'édition 2013, le rapport a été étendu pour inclure une section sur les canaux latéraux de matériel informatique et de logiciels, la génération de nombres aléatoires, une gestion clé de la durée de vie, alors que la partie sur les protocoles est étendue pour 2014 et est une étude indépendante sur les protocoles cryptographiques.

Le rapport explique deux aspects des mécanismes cryptographiques :

- Si des données primitives ou un programme peuvent être envisagés pour être utilisés actuellement, dans le cas où ils sont déjà déployés ;
- si des données primitives ou un programme conviennent en vue d'un déploiement dans des systèmes nouveaux ou à venir.

Les questions de conservation des données à long terme sont analysées avec un nombre de problèmes généraux liés au déploiement des données primitives et des programmes. L'ensemble des mécanismes abordés dans ce rapport sont jusqu'à un certain point normalisés, et ils ont été soit déployés ou il est prévu de les déployer, dans les systèmes réels.

« Étude sur les protocoles cryptographiques »

Le second rapport se concentre sur le statut actuel dans les protocoles cryptographiques et encourage une recherche plus approfondie. Un bref aperçu est présenté sur les protocoles qui sont utilisés dans des domaines d'application relativement limités, tels que le domaine sans fil, les communications mobiles, le domaine bancaire ((Bluetooth, WPA/WEP, UMTS/LTE, ZigBee, EMV) et des environnements spécifiques mettant l'accent sur le « cloud computing ».

L'accent principal du rapport porte sur les directives aux chercheurs et aux organisations dans le domaine, qui comprennent :

- Les protocoles de sécurité et cryptographiques, qui doivent être conçus par les experts en matière de protocole cryptographique, plutôt que jusqu'à présent par le réseautage et les experts en matière de protocole. De plus, les chercheurs doivent simplifier l'analyse et
- permettre aux outils automatisés pour fournir des garanties informatiques solides.
- Une attention plus soutenue requise pour la vérification automatisée, afin que la mise en œuvre d'un protocole puissent répondre aux objectifs en matière de sécurité, et examine la manière dont les outils automatisés peuvent garantir la mise en œuvre correcte de la conception d'un protocole.
- De petits changements insignifiants dans les protocoles peuvent avoir pour effet l'invalidation des preuves de garantie.
- Les protocoles futurs doivent être conçus en utilisant des principes d'ingénierie solides et bien établis, faciliter l'analyse de sécurité officielle, et en conjonction avec des preuves de sécurité officielle, conçus dans la cryptanalyse de leurs constituants primitifs.
- Les protocoles futurs ne doivent plus être plus complexes qu'ils n'ont besoin de l'être.
- De plus amples travaux doivent être réalisés sur la vérification des API pour les protocoles d'application.

Udo Helmbrecht a déclara à propos de ce rapport: *« Ce qui est mis en exergue est le besoin de programmes de certification dans toutes les phases du cycle de vie technologique. Les processus et les produits intégrés de "sécurité par la conception ou par défaut", sont des principes de base pour la confiance. La normalisation des processus est un élément essentiel dans l'assurance de l'application correcte de la réforme de protection des données dans le service aux citoyens européens et son marché intérieur. Les directives de l'ENISA s'efforcent de fournir le cadre adéquat dans la sécurisation des systèmes en ligne. »*

Le règlement CE 611/2013 référence l'ENISA en tant que corps consultatif, dans le processus d'établissement d'une liste des mesures de protection cryptographiques appropriée pour la protection des données personnelles. Les directives cryptographiques de l'ENISA doivent servir de documents de référence. Dans cette optique, les principes directeurs sont relativement conservateurs, fondés sur la recherche de pointe actuelle, en abordant la construction de nouveaux systèmes commerciaux avec un long cycle de vie.

Pour les rapports complets : « Algorithmes, taille clé et paramètres » & « Étude sur les protocoles cryptographiques »

Pour les entretiens et plus d'informations press[at]enisa.europa.eu