Newsletter N°3/2014

RESTENA
Réseau Téléinformatique de l'Education Nationale et de la Recherche

Informations sur le déroulement d'une enquête lors d'une cyberattaque et quelques recommandations.

D'UNE CYBERATTAQUE À LA SAISIE DES DONNÉES

Les incidents et attaques liés à la sécurité informatique, appelés cyberattaques, deviennent plus nombreux de ces jours. La nature d'une cyberattaque ainsi que les conséquences d'une telle peuvent être très diversifiées.

Ces attaques peuvent être de simples messages non-sollicités (« spam ») mais également s'étendre jusqu'à des piratages virulents et complexes (virus, cheval de Troie,...) ayant des conséquences sévères et coûteuses, comme l'indisponibilité du système ainsi que la perte de données sensibles.

Lors d'une cyberattaque, il est conseillé aux victimes de la rapporter auprès d'une autorité légale et de déposer plainte dans les meilleurs délais afin de permettre la sauvegarde des traces et la recherche de preuves.

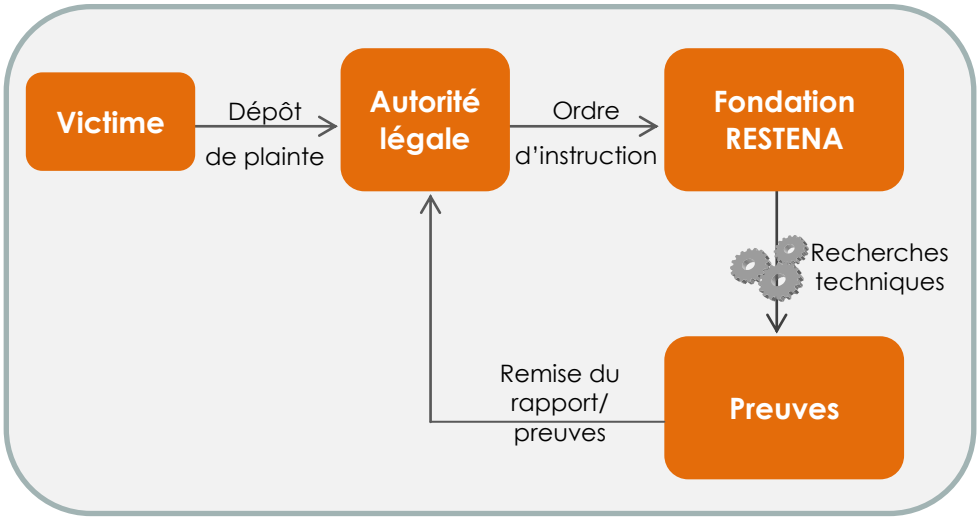

Figure: Procédure pour une saisie de données

Ce document décrit les procédures suivies par la Fondation RESTENA pour répondre à une demande d'informations de la part d'une autorité légale suite à une instruction judiciaire. De plus, il donne quelques recommandations aux institutions victimes d'une attaque pour contribuer au bon déroulement d'une enquête.

Fondation RESTENA
6, rue Richard Coudenhove-Kalergi
L-1359 Luxembourg
Tél: +352 4244 09-1
Fax: +352 42 24 73

Conformément à la loi luxembourgeoise, une autorité légale comme la police de proximité, la police judiciaire ou le parquet luxembourgeois, peut saisir des données et autres preuves auprès des opérateurs et fournisseurs de services électroniques dans le cadre d'une enquête.

Dès le dépôt d'une plainte par la victime, une instruction pour la perquisition des données est ouverte. Celle-ci est remise à l'opérateur ou au fournisseur de services électroniques concerné.

Quand la Fondation RESTENA se voit confrontée à une telle situation, elle supporte l'enquête techniquement et se charge de la recherche de preuves afin de garantir que la saisie des données se déroule selon les règles de l'art.

Les données requises par une enquête incluent des données relatives au trafic, comme les données de transition qui sont composées des adresses IP, des ports, de la date et de l'heure, de la durée de la communication, des protocoles utilisés, etc. Les données relatives au trafic peuvent en général être retracées jusqu'au compte de l'utilisateur de l'entité concernée.

La loi luxembourgeoise de juillet 2010* prévoit que les fournisseurs de services électroniques et les opérateurs conservent les données relatives au trafic pour une durée d'au moins six mois à compter de la date où la communication a eu lieu.

Il est donc vivement conseillé aux victimes de déposer plainte au plus vite pour éviter l'effacement des données, donc des preuves, si la période de six mois est dépassée.

Informations sur les autorités légales au Luxembourg

a) Police Grand-ducale du Luxembourg

b) Parquet du Luxembourg
– Parquet du Tribunal d'Arrondissement du Luxembourg
– Parquet du Tribunal d'Arrondissement de Diekirch

c) Service de la Police Judiciaire, Section Nouvelles Technologies, Luxembourg

*: Loi du 24 juillet 2010 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle.

Comment contribuer efficacement à une enquête en tant qu'institution?

- Gardez à jour vos coordonnées institutionnelles ainsi que, le cas échéant, celles de votre contact de sécurité. Ceci facilitera la prise de contact lors d'une cyberattaque sur votre réseau. Si vous avez besoin d'aide pour mettre à jour les détails de vos coordonnées signalétiques, contactez la Fondation RESTENA.

- La loi luxembourgeoise exige de certaines institutions en fonction de leur activité de disposer d'un système de journalisation. En général, il est conseillé de disposer d'un tel système archivant des données relatives au trafic du réseau informatique. Ceci facilitera la réponse technique aux requêtes lors d'une enquête.

- Mettez en place une procédure qui décrit les différentes démarches à suivre lors d'une enquête auprès de votre institution. Avec des procédures bien définies, vous ne freinez pas l'enquête car les responsabilités et les différents rôles sont bien définis.

- Informez la direction de votre institution sur les différentes procédures en place pour répondre à une enquête.

- En tant que victime d'une cyberattaque, portez immédiatement plainte. Si vous disposez d'un système de journalisation des données relatives au trafic sur votre réseau, conservez toutes les évidences possibles sur toute la durée de l'attaque et joignez-les à votre plainte.

Confidentialité des données

De manière générale et en se référant à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel[+], la Fondation RESTENA ne communique en aucun cas des données sensibles respectivement des données relatives au trafic sur sa communauté à une partie tierce. Les données sensibles sauvegardées ne sont ni utilisées à des fins commerciales ni à des fins de surveillance.

Seule exception : une enquête officielle menée par une autorité légale. Dans ce cas, seulement les données relatives à l'incident sont communiquées.

[+]: Dernière modification: Loi du 28 juillet 2011 sur la protection des données dans le secteur des communications électroniques. Mémorial A N°172 du 10 août 2011

RESTENA - CSIRT
Computer Security Incident Response Team

Le RESTENA-CSIRT se présente

RESTENA-CSIRT (angl.: **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam) est l'équipe de réponse aux incidents de sécurité informatique et le point de contact pour le traitement d'incidents informatique de la communauté de l'éducation et de la recherche.

La mission de RESTENA-CSIRT est de soutenir et de coordonner la réponse aux incidents de la sécurité informatique dans sa communauté ainsi que de servir comme organe de confiance et point de contact pour la demande d'informations relatives aux incidents de sécurité.

Un autre objectif est de sensibiliser et d'instruire sa communauté sur l'importance de la sécurité dans le domaine de l'IT et du web.

Lien vers la page web: www.restena.lu/csirt

Contact: csirt@restena.lu

Si vous avez d'autres questions relatives aux cyberattaques ou sur la sécurité informatique, veuillez vous adresser au helpdesk ou au CSIRT.

helpdesk@restena.lu ou csirt@restena.lu

Ou par téléphone au: +352 42 44 09 - 1