Newsletter N°3/2014

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

Information about the procedure of data acquisition in case of a cyber-attack and some recommendations.

FROM A CYBER-ATTACK TO DATA ACQUISITION

Computer security incidents and attacks, also called cyber-attacks, become numerous on these days. The nature of a cyber-attack can be diversified, the same as for the related consequences.

This can range from simple unsolicited bulk-mail up to complex and sophisticated piracies (virus, Trojan horse...). Commonly such attacks result in strong and costly consequences such as the complete system failure or the loss of sensitive data.

In case of a cyber-attack, it is recommended to the victim to report it next to a legal authority and to file charges as quickly as possible such that proofs and traces can be recovered and preserved.

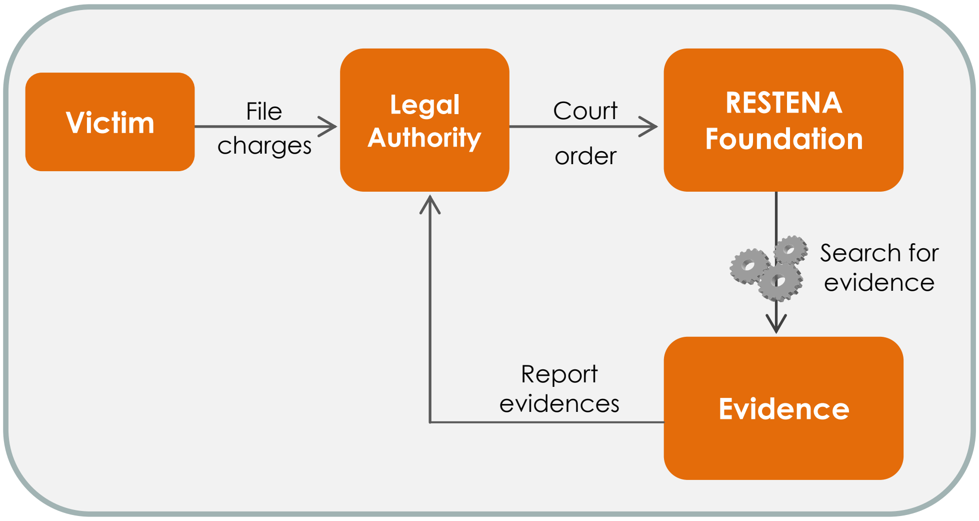

Figure: Procedure to be followed for securing evidence

This document describes the procedure respected by the RESTENA Foundation to comply with an information request by a legal entity in the framework of an investigation. The more, it gives some recommendations to attacked institutions on how to support an investigation practically.

Fondation RESTENA

6, rue Richard
Coudenhove-Kalergi

L-1359 Luxembourg

Tél: +352 4244 09-1

Fax: +352 42 24 73

Conform to Luxembourgish law, a legal entity such as the local police, the criminal police or the public prosecutor can collect evidence and other proofs next to operators and electronic service providers in the framework of an investigation.

After the victim has filed charges, a court order to proceed to take evidence is opened. It is then handed to the operator or to the electronic service provider concerned by the cyber-attack.

When being confronted to such a situation, the Foundation supports the investigation practically. It takes care of the technical search for proofs in a way that the collection and securing of evidences respects state of the art techniques.

The requested data includes data related to traffic, such as IP-addresses, ports, date and time, duration of the communication, protocols and so on. In general, data related to traffic enables to trace back to the personal /user account of the responsible entity.

Luxembourgish law from July 2010* states that operators or electronic service providers have to archive data related to traffic for at least six months starting from the date where a communication has occurred.

In case of a cyber-attack, it is recommended to file charges as quickly as possible next to a legal authority to avoid deletion of suspect data respectively proofs after this period of six months.

Information about legal authorities in 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.

How to effectively contribute to an investigation as an institution?

- Keep your institutional contact information respectively your security contact up to date. This eases contacting you in case of a cyber-attack on your network. If you need help to update your contact information, please contact the RESTENA Foundation.

- Luxembourgish Law requests some institutions, depending of their business to have a logging system for data related to network traffic in place. In general, it is advisable to all kind of institution to have such a network monitoring system in place to log network traffic. This simplifies the technical response to an investigation.

- Put a procedure in place that clearly describes the steps to respect in your institution in case of a request by a legal authority. With a procedure in place you do not delay the investigation since responsibilities and roles are well-defined.

- Ensure that your management is aware about the procedures in place for responding to investigations.

- In case of being a victim of a cyber-attack, immediately file charges next to a legal entity. If you have a network monitoring system in place, store and preserve evidence and logs related to network traffic for the period of the attack and join them to your file.

Data confidentiality

Referring to the modified law of August 2nd, 2002, relating to the protection of the person with regard to the processing of personal data+, the RESTENA Foundation will never communicate any sensitive information or information related to traffic about its user community to a third party. Stored sensitive data will not be given to third parties neither for commercial nor for surveillance purpose.

The only exception: an investigation by a legal authority. In this case, only information about the cyber-attack are disclosed.

+: Last 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

Presenting the RESTENA-CSIRT

The RESTENA-CSIRT is the **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam of the RESTENA Foundation and the contact point for the handling of security incidents affecting the education and research community.

The mission of the RESTENA-CSIRT is to support and coordinate the security incident response within its constituency, to serve as a trusted point of contact and to act as clearing house for security incident-related information.

Another aim of the RESTENA-CSIRT is to increase the awareness and knowledge about IT security among its constituents.

Link to the website: www.restena.lu/csirt

Contact: www.restena.lu/csirt

If you have further questions about cyber-attacks or related to computer security, please contact the RESTENA helpdesk or the CSIRT team.

helpdesk@restena.lu or csirt@restena.lu

Or by phone: +352 42 44 09 - 1