Tip sheet

FROM A CYBERATTACK TO DATA ACQUISITION

Computer security incidents and attacks, known as cyberattacks, are on the rise. Both the nature of a cyberattack and its consequences can be very diverse. From simple unsolicited messages (spam) to virulent and complex hacking (viruses, Trojan horses, etc.), the consequences can be strong and costly, with among the most important one for an institution: the unavailability of an entire system and the loss of sensitive data.

Procedures and legal investigation

Filing a complaint with a legal authority

Any person or institution that is a victim of a cyberattack is invited to report the attack to a legal authority and to file a complaint as quickly as possible. This rapid action allows both the preservation of traces and the search for evidence.

In accordance with Luxembourg law, a legal authority such as the local police, the criminal police or the public prosecutor can collect evidence and other proofs from operators and electronic service providers in the context of an investigation.

As soon as a complaint is filled by the victim, a court order for the search of data is opened. It is then handed to the operator or the electronic service provider concerned by the cyberattack.

Procedure to be followed for securing evidence

Supporting investigation

Providing access to the research and education network, the Restena Foundation can be requested by a legal authority. In this case, the Restena Foundation technically supports the investigation and is in charge of searching for evidence.

The data requested for an investigation includes traffic data, such as transition data consisting of IP-addresses, ports, date and time, duration of the communication, protocols, etc. Traffic data can usually be traced back to the personal/user account of the responsible entity.

The Luxembourg law of July 2010* states that both electronic service providers and operators have to archive traffic data for a period of at least six months starting from the date on which a communication has occurred. Victims are therefore strongly advised to file a complaint as quickly as possible in order to avoid the deletion of data, and therefore of evidence, if the six-month period is over.

Legal authorities in Luxembourg

- Police Grand-ducale du Luxembourg
- Parquet du Luxembourg (Parquet du Tribunal d'Arrondissement du Luxembourg et Parquet du Tribunal d'Arrondissement de Diekirch)
- Service de la Police Judiciaire, Section Nouvelles Technologies, Luxembourg

** Law of 24 July 2010 amending Articles 5 and 9 of the amended Law of 30 May 2005 on the protection of privacy in the electronic communications sector and Article 67-1 of the Code of Criminal Procedure.*

restena
réseau · sécurité · .lu

Effectively contribute to an investigation

Any institution may be confronted with cyberattacks. It is important to be prepared for this eventuality so that you can contribute to a successful investigation. To do this, we give you a few simple recommendations.

Keep your institutional and/ or security contact information up to date.

Up-to-date contact information makes it easier to get in touch in case of a cyberattack on your network. If you need help to update your contact information, contact the Restena Foundation.

Set up a logging system.

By archiving computer network traffic data, a logging system makes it easier to technically respond to queries during an investigation. Luxembourg law requires certain institutions, depending on their activity, to have such a system in place.

Establish a procedure describing actions to be taken in the course of an investigation.

Thanks to clear procedures defining both responsibilities and roles of each person, you will not hinder the investigation in progress.

Immediately fill a complaint if you are the victim of a cyberattack.

If you have a system for logging traffic data on your network, keep all possible evidence throughout the attack and attach it to your complaint.

Data confidentiality

In general, and with reference to the regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data, GDPR in progress**, the Restena Foundation does not, under any circumstances, communicate traffic data on its community to a third party. Those sensitive data are neither used for commercial purposes nor for monitoring purposes.

Exception: In the context of an investigation by a legal authority, only information about the cyberattack are disclosed.

→ Your institution is the victim of a cyberattack?
Do not wait any longer, react immediately!

Service offer

Thanks to its Computer Security Incident Response Team (Restena-CSIRT), the Restena Foundation assists the Luxembourg's research and education community encountering computer security incidents.

For more information on this service, please visit www.restena.lu/csirt

*** Regulation 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, that repeals Directive 95/46/EC (General Data Protection Regulation).*

restena
réseau · sécurité · .lu