

Luxembourg Country Report



About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

Contact details

For contacting ENISA or for general enquiries on the Country Reports:

Mr. Giorgos Dimitriou

ENISA External Relations Expert

Giorgos.Dimitriou@enisa.europa.eu

Internet: <http://www.enisa.europa.eu>



Acknowledgments:

ENISA would like to express its gratitude to the National Liaison Officers that provided input to the individual country reports. Our appreciation is also extended to the ENISA experts and Steering Committee members who contributed throughout this activity.

ENISA would also like to recognise the contribution of the Deloitte team members that prepared this country report on behalf of ENISA: Vincent **Bouckaert**, **Dan Cimpean**, **Johan Meire** and **Nicolas Roosens**.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as amended by Regulation (EC) No 1007/2008. This publication does not necessarily represent state-of-the-art and it might be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication. Member States are not responsible for the outcomes of the study.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. Reproduction is authorised provided the source is acknowledged.

© European Network and Information Security Agency (ENISA) 2011

Table of Contents

LUXEMBOURG	4
THE STRUCTURE OF THE INDIVIDUAL COUNTRY REPORTS	4
NIS NATIONAL STRATEGY, REGULATORY FRAMEWORK AND KEY POLICY MEASURES	5
OVERVIEW OF THE NIS NATIONAL STRATEGY	5
THE REGULATORY FRAMEWORK	5
NIS GOVERNANCE	9
OVERVIEW OF THE KEY STAKEHOLDERS	9
INTERACTION BETWEEN KEY STAKEHOLDERS, INFORMATION EXCHANGE MECHANISMS IN PLACE, CO-OPERATION & DIALOGUE PLATFORMS AROUND NIS	10
FOSTERING A PROACTIVE NIS COMMUNITY	12
COUNTRY-SPECIFIC NIS FACTS, TRENDS, GOOD PRACTICES AND INSPIRING CASES....	13
SECURITY INCIDENT MANAGEMENT	13
EMERGING NIS RISKS	13
RESILIENCE ASPECTS	14
PRIVACY AND TRUST	15
NIS AWARENESS AT THE COUNTRY LEVEL	16
RELEVANT STATISTICS FOR THE COUNTRY	18
INTERNET ACCESS OF POPULATION AND ENTERPRISES	18
STATISTICS ON USE OF INTERNET BY INDIVIDUALS AND RELATED SECURITY ASPECTS	19
STATISTICS ON USE OF INTERNET BY ENTERPRISES AND RELATED SECURITY ASPECTS	20
OTHER STATISTICS	21
APPENDIX	22
NATIONAL AUTHORITIES IN NETWORK AND INFORMATION SECURITY	22
COMPUTER EMERGENCY RESPONSE TEAMS (CERTs)	25
INDUSTRY ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	27
ACADEMIC ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY BODIES	28
OTHER BODIES AND ORGANISATIONS ACTIVE IN NETWORK AND INFORMATION SECURITY	29
REFERENCES	29

Luxembourg

The structure of the individual country reports

The individual country reports (i.e. country-specific) present the information by following a structure that is complementary to ENISA's "Who-is-who" publication and is intended to provide additional value-added to the reader:

- *NIS national strategy, regulatory framework and key policy measures*
- *Overview of the NIS governance model at country level:*
 - *Key stakeholders, their mandate, role and responsibilities, and an overview of their substantial activities in the area of NIS:*
 - *Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS*
 - *Fostering a proactive NIS community*
- *Country specific NIS facts, trends, good practices and inspiring cases:*
 - *Security incident management*
 - *Emerging NIS risks*
 - *Resilience aspects*
 - *Privacy and trust*
 - *NIS awareness at the country level*
- *Relevant statistics for the country.*

This report is based on information which was publicly available when research was carried out, as well as comments received from National Liaison Officers and ENISA experts. As such, the country report presents a high-level snapshot of NIS at the turn of the year.

NIS national strategy, regulatory framework and key policy measures

Overview of the NIS national strategy

The Luxembourg national NIS strategy was agreed upon and launched in 2003 by the Ministry of the Economy and Foreign Trade. No major change of the NIS strategy has been realized in 2010. The current NIS strategy remains built on four main pillars:

- Sensibilisation and prevention (CASES): Raising awareness, development of preventive skills and building up of trust;
- Intervention (CIRCL): preservation of sovereignty during incidents and development of curative skills;
- Investigation: Preservation of sovereignty, development of better investigative skills and development of better forensic skills.

Legislation: Defence of the Luxembourgish interests, keeping up with European laws and building up of a legal framework favourable to economics and finance.

IT Strategy and the “eGovernance”

In order to increase the visibility of the public services, a strategy¹ to use ICT by the public authorities has been defined. In the context of the growing prevalence of online public services in the state-citizen relationship, the eGovernment strategy in Luxembourg is based on the Standardisation Charter for the presence of the State on the Internet (“ReNo: Référentiel de normalisation pour les sites web du Gouvernement”, see: www.eluxembourg.lu).

The portal of the Luxembourg administrative authorities (www.guichet.lu) describes the most common procedures and makes available the forms relating thereto, allowing for certain procedures to be carried out online. Procedures concerning citizens as well as companies are covered by this portal.

The regulatory framework

eGovernment Act

There is currently no overall eGovernment legislation in Luxembourg. But the new version of the eGovernment Action Plan² has been adopted. Among other things, the government’s strategy to move away from ‘vanity sites’ and towards portals has been officialised by the plan which will, for instance, integrate the descriptions of the different ministries and administrations into the [gouvernement.lu](http://www.gouvernement.lu) portal, which is in the process of being redesigned.

In addition, an internal audit/benchmark of the government’s Internet presence as a whole (‘Baromètre de la qualité des presences Internet de l’Etat’) is in its final stages and its results will be published later on this year. Finally, a Business Process Management Office (BPMO) has been set up and is currently analysing and mapping the internal processes of different administrations.

¹ Source: http://ec.europa.eu/information_society/activities/ict_psp/documents/ict_psp_wp2009.pdf

² See : http://www.epractice.eu/files/eGov%20in%20LU%20-%20May%202010%20-%202013.0_0.pdf

Data Protection/Privacy Legislation

The amended Data Protection Act³ of 2 August 2002, is governing the processing and use of personal data in Luxembourg (implementation of the EU Data Protection Directive 1995/46/EC).

The 'Processing of Personal Data in the Electronic Communications Sector' Act, adopted on 30 May 2005 and which entered into force on 1 July 2005, transposes the EU Directive on privacy and electronic communications (2002/58/EC). This Act forms part of Luxembourg's legislative 'Paquet Telecom' (See eCommunications legislation subsection of the present section). It aims at protecting the privacy of Internet users (including protection against unsolicited commercial communications or 'spam') and users of services with added value such as the GPS.

The data protection authority, National Commission for Data Protection (CNPD) created by the 2002 Data Protection Act, remains competent for checking the legality of the processing of personal data.

eCommerce Legislation

The eCommerce Act⁴ of 14 August 2000 (modified 5.07.2004) transposes among other the EU eCommerce Directive (2000/31/EC).

The payment services act of 10th Novembre 2009, transposes the European directive 2007/64/CE. This act amends the eCommerce Act as well as the Data Protection Act.

eCommunications Legislation

The new eCommunications Law⁵ of 30 May 2005 transposes the EU regulatory framework for electronic communications (Directives 2002/19/EC, 2002/20/EC, 2002/21/EC, 2002/22/EC). This law forms part of Luxembourg's legislative 'Paquet Telecom' which also includes a specific law on the processing of personal data in the electronic communications sector (see Data Protection/Privacy legislation subsection of the present section).

We notice here that the major update that has happened in 2010 is the approval of the article 13a related to the "Telecom package".

The eCommunications Law notably regulates access to electronic communications networks as well as their interconnection, so as to allow a long-lasting competitive environment in this sector and interoperability of eCommunications services while bringing benefits to consumers. It also sets out the rights of the users, the obligations of the services and network providers thus defining the 'universal service notion as regards eCommunications.

Cybercrime legislation

Most of the current cyber-crime provisions were introduced by the Law of 15 July 1993⁶ combatting economical crime and IT fraud (Loi tendant à renforcer la lutte contre la criminalité économique et la fraude informatique), and were incorporated in the Luxembourg Penal Code. The majority of the relevant provisions can be found in Title IX, Section VII of the second book of the Penal Code, entitled "Regarding certain ICT violations (De certaines infractions en matière informatique), and in several provisions related to telecommunication protection. Available

³ Source: <http://www.epractice.eu/files/eGovernment%20in%20LU%20-%20May%202009%20-%202011.0.pdf>

⁴ Source: <http://www.epractice.eu/files/eGovernment%20in%20LU%20-%20May%202009%20-%202011.0.pdf>
– the same source was used for several other laws in this section

⁵ <http://www.epractice.eu/files/eGovernment%20in%20LU%20-%20May%202009%20-%202011.0.pdf>

⁶ See: ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf

provisions focus mostly on unauthorized intrusions and damage resulting from such intrusions, ICT fraud, and the obstruction of the proper functioning of computer systems.

Relevant case law is largely unavailable, so that it is difficult to judge the efficiency of the current legislation.

The Police Corps and the Gendarmerie were merged as of 1 January 2000 to form the Police Grand-Ducale, which carries out all police functions throughout the Grand Duchy. It is under the authority of the Ministry of the Interior, and contains a number of services, including the Judicial Police Service (Service de Police judiciaire). This service is divided in a number of specialized sections, including the New Technologies section, which assists the investigating magistrate (*juge d'instruction*) in criminal investigations when required.

Criminal jurisdiction of Luxembourg has been attributed to four major courts: the Police Court (Tribunal de Police), the Criminal or Correctional Chamber of the Regional Court, (Tribunal d'Arrondissement, Chambre criminelle/correctionnelle), the Criminal Chamber of the Court of Appeal (Cour d'Appel, Chambre criminelle) and the Supreme Court (Cour de Cassation). The court most likely to deal with computer crime is the Criminal Chamber of the Regional Court.

Against its decisions, appeal can be lodged with the Court of Appeal (Cour d'Appel). The Supreme Court (Cour de Cassation) only hears points of law. Proceedings on the merits of the case are always preceded by an inquiry under the supervision of the investigating magistrate (*juge d'instruction*). Some of the relevant incidents are:

- Target Fingerprinting;
- Malicious code;
- Denial of service;
- Account compromise;
- Intrusion attempt;
- Unauthorised access to information;
- Unauthorised access to transmissions;
- Unauthorised modification of information;
- Unauthorised access to communication systems;
- Spam.

Since beginning of 2010 no update of the cybercrime legislation has been identified for Luxembourg.

eArchiving

Luxembourg is currently working on the new eArchiving Act that is meant to regulate the electronic archiving of documents as well as the accreditation scheme for eArchiving professional.

Self-regulations

There is currently no overall self-regulation legislation in Luxembourg.

eIdentity

General overview

Luxembourg uses private sector smart cards (LuxTrust cards) for all natural and legal persons. Some non-card identity tokens are also used (the LuxTrust Signing Stick - USB stick with two digital certificates).

Luxembourg initiated an e-Government applications project which relies on a PKI system (users authenticate themselves with the LuxTrust certificates). LuxTrust includes Signing Server Certificate, SSL and Object Signing Certificates, Trusted Time Stamp and Tailor Made LuxTrust Solutions.

Non PKI-based systems are also used in this country, such as the eTVA application which allows a user to submit VAT tax declarations. A simple username/password system establishes the electronic authentication, based on prior authorization after a (handwritten) application form submitted by the user to the authorities.

Luxembourg is also active member of the European project STORK⁷ (Secure idenTity acrOss borders linKed) that is aimed at enabling businesses, citizens and government employees to use their national electronic identities in any Member State.

The consortium members include national authorities, non profit organisations, private companies and academic partners from: **Austria, Belgium, Estonia, France, Germany, Italy, Luxembourg, Netherlands, Portugal, Slovenia, Spain, Sweden, United Kingdom and Iceland.**

eSignatures legislation

Luxembourg was the first European country to implement the guidelines on trade and the electronic signature, leading to the Law on Electronic Commerce August 14, 2000, followed by the establishment of a quality label "Luxembourg e-commerce certified". The eCommerce Law of 14 August 2000 is complemented by a regulation of 1 June 2001 on electronic signatures and electronic payments. No major updates to this eSignature legislation have been noticed in 2010.

⁷ The STORK project consortium consists of 29 participants representing 13 Member States and Iceland. A full list of participants in the STORK project is available at www.eidstork.eu

NIS Governance

Overview of the key stakeholders

We included below a high-level overview of the key actors with relevant involvement, roles and responsibilities in NIS matters.

National Authorities	<ul style="list-style-type: none"> • Direction of the electronic trade and information security in the Ministry of the Economy and Foreign Trade • Cyberworld Awareness and Security Enhancement Structure (CASES) • BEE SECURE • "Security made in Lëtzebuerg" (SMILE) • Commissionership of the national protection - Haut Commissariat a la Protection Nationale (HCPN) • Ministerial Council of the national protection - Conseil Ministériel de la Protection Nationale (CMPN) • National committee of telecommunications - Comité national des Télécommunications (CONATEL) • National committee of critical infrastructure - Comité national de l'infrastructure critique (CONATIC) • Regulatory institution of the Luxembourg - Institut Luxembourgeois de Régulation (ILR) • Centre of Technologies and information for the national government - Centre des Technologies de l'Information de l'Etat (CTIE) • National commission of the data protection - Commission National pour la Protection de Données (CNPD) • Communication centre of the government - Centre de communication du government (CGC) • Service of media and communication - Service des Medias et de la Communication (SMC) • National regulator for the financial sector - Commission de surveillance du Secteur Financier (CSSF) • National Education and Research Network - Réseau Téléinformatique de l'Education Nationale et de la Recherche (RESTENA) • Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services (ILNAS) • Consumer Association of Luxembourg - Union Luxembourgeoise des Consommateurs (ULC) • Centre Européen des consommateurs (CEC)
CERTs	<ul style="list-style-type: none"> • CIRCL • RESTENA-CSIRT • ASBL CSRRT-LU
Industry Organisations	<ul style="list-style-type: none"> • Internet Society in Luxembourg (ISOC) • Professional association of Information Security - Association des Professionnels de la Société de l'Information (APSI) • Fedil - Business Federation Luxembourg • CLUSIL
Academic Organisations	<ul style="list-style-type: none"> • Laboratory of Algorithmic, Cryptology and Security (LACS) (at the University of Luxembourg) • Interdisciplinary Centre for Security, Reliability and Trust (at the University of Luxembourg) • Public Research Centre Henri Tudor • Public Research Centre Gabriel Lippmann
Others	<ul style="list-style-type: none"> • ISACA LU • OWASP – Luxembourg local chapter • Syn2cat • Luxtrust

For contact details of the above-indicated stakeholders we refer to the ENISA "Who is Who"⁸ – 2010 Directory on Network and Information Security and for the CERTs we refer to the ENISA CERT Inventory⁹.

NOTE: only activities with at least a component of the following eight ENISA focus points have been taken into account when the stakeholders and their interaction were highlighted: CERT, Resilience, Awareness Raising, Emerging Risks/Current Risks, Micro-enterprises, e-ID, Development of Security, Technology and Standards Policy; Implementation of Security, Technology and Standards.

Interaction between key stakeholders, information exchange mechanisms in place, co-operation & dialogue platforms around NIS

Co-operation via the Ministry of the Economy on advanced technologies

The Ministry of Economy has created in 2002 an "InfoCom cluster" grouping ICT companies of various sizes and sectors, cooperating transversely (market research, R&D) on advanced technologies (wireless, satellite, multimedia ...). This initiative, led by Luxinnovation, is an endogenous development of the economy and dissemination of experiences to the entire market.

Co-operation via the national regulator for crisis prevention and management

Telecom Operators have to provide quality indicators to the national regulator, called "Institut Luxembourgeois de Régulation" (ILR). These statistical reports cover availability aspects, coverage and incident reports. Most reports have to be delivered on a yearly basis.

The national contact for Internet service providers and for ENISA, in the context of the Art. 13a of Telecom Package will be the ILR.

The new law for the National Protection Structure will introduce a mandatory mechanism for the exchange of information between providers and public authorities. This exchange comprises all information necessary for crisis prevention and management. Presently operators exchange incident information on a sporadic basis with governmental services (HCPN). This exchange is already put into place but is performed in the case of serious incidents, such as network overload due to SMS flooding on peak times as it happened once on Sylvester.

Moreover, ILR and operators meet on a regular basis. The main topic on the agenda is not network resilience, but market regulation. The CCG, has together with the main Luxembourg operator implemented crisis communication handling in the terrestrial telephone network. This has been done via a common resilience improvement project.

Information exchange via CASES and CIRCL

The governmental structure CASES is promoting awareness, it showcases best practice in the area of IT security for citizens, SME and government. (Protection of the nodes protects the communication channels between these nodes). CASES meets with operators on regular basis. With the main operator, implementation of awareness between respective customers and

⁸ The ENISA Who-is-Who Directory on Network and Information Security (NIS) contains information on NIS stakeholders (such as national and European authorities and NIS organisations), contact details, websites, and areas of responsibilities or activities. Ref. code: ISBN 978-92-9204-003-1 - Publication date: May 12, 2010

⁹ See: <http://www.enisa.europa.eu/act/cert/background/inv/certs-by-country/>

employees is ongoing. CASES publishes best practice in various areas, which can be adopted by the private sector.

The private sector presently cannot be forced to adopt measures. There is no regulator checking the implementation. Only the financial sector (together with sub-contractors) has to apply to security standards defined by the banking supervision authority CSSF.

CASES works closely with the Ministry of Families, the Ministry of Education, the Ministry of Interior, the SIGI (local government IT department), the SNJ (National youth department) and the Police in the area of awareness raising of youth and adolescents.

In recent years CASES has managed to acquire several partnerships with foreign governmental organizations with similar awareness raising missions. For instance CASES has a strong cooperation with the new service of the French agency ANSSI on public awareness.

The national CERT, CIRCL forwards information on specific vulnerabilities or threats to the national operators. This is not done on a regular, but on a spontaneous basis. CIRCL attends meetings of TF-CSIRT¹⁰, FIRST¹¹ and other international forums, developing important partnerships for the resolution of incidents and the exchange of specific information.

Furthermore CIRCL has set up an information sharing platform with the industry, telecom and bank sector in 2010.

Information exchange managed via smile GIE

Once a year, the CASES & CIRCL together organize hack.lu (an IT security conference). This conference focuses on different aspects of IT security and brings together experts from government and from the private sector.

Other co-operation of NIS stakeholders

ILNAS organizes the standardization work, by the in-house Luxembourg's standards body, and supports particularly the development of the standardization work in the field of Information Technology (ISO/IEC/JTC1), by the in-house Digital Trust Department, notably registers a strong national technical committee dedicated to Information Security (ISO/IEC/JTC1/SC27).

Furthermore there are very active information security organizations, such as CLUSIL, OWASP, ISACA, etc. where stakeholders from the academic world, the public sector and the private sector come together to share knowledge and best practices regarding various NIS topics.

Interaction between governmental authorities on national network resilience aspects

The HCPN, the associated national Committees and the CCG have capabilities for crisis management¹². The government as such, advised by CONATEL and CONATIC, has the possibility, in the case of a national crisis or a catastrophe, to requisition, for a limited period and following the principle of proportionality, public networks. Incidents are collected and analysed by CIRCL and are also fed into the CASES (awareness raising node in Luxembourg). CIRCL's approach is based upon the common recommendations existing for CERTs.

¹⁰ See: <http://www.terena.org/activities/tf-csirt/>

¹¹ See: <http://www.first.org>

¹² See: <http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies>

Information exchange platform via Academic organisations

At the University of Luxembourg, the Interdisciplinary Centre for Security, Reliability and Trust provides a meeting place in Luxembourg for knowledge transfer and exchange of ideas with a special focus on small and medium sized businesses.

The Public Research Centre Henri Tudor informs the private and public sectors regarding the progress and projects in ICT innovation via scientific and professional conferences.

Fostering a proactive NIS community

Amongst the most visible initiatives:

- CIRCL, the national CERT, has gained widespread reputation among the CERT community and has become the contact point in Luxembourg for incident reporting and handling.
- The Hack.lu conference in Luxembourg attracts yearly an international community of security researchers and specialists.
- CASES shares it's knowledge and experience about awareness raising amongst partner organisations in Europe.
- BEE SECURE is the Luxembourg node of the European Safer Internet Programme.

Country-specific NIS facts, trends, good practices and inspiring cases

Security incident management

It was noted that security incident information and data are collected through different channels (e.g. CIRCL, CTIE, etc). Though, no statistic or reporting is available for the public.

The recent law for the National Protection Structure introduces a mandatory mechanism for the exchange of information between providers and public authorities. This exchange encompasses all information necessary for crisis prevention and management. Within governmental networks, incidents are handled by the CCG, the CTIE and CIRCL. CIRCL currently liaises with each of the government departments on the basis of one or two contact persons for reporting incidents (trusted partner within the administration).

The incidents are reported via telephone, e-mail or fax according to a form which is designed for incident reporting. A setup of system sensors that are constantly watching the network is also planned, so that strange behaviour in the network triggers alarms and necessary steps are taken to react efficiently and in a timely manner. Operators report on a voluntary basis. Serious incidents have to be reported to the national authorities (including regulators), such as it happened once the overload of SMS networks on Sylvester's eave.

In terms of security incident management no significant changes have been identified in comparison with previous year report.

Emerging NIS risks

The national risk management process

A national risk management process¹³ is still under development by HCPN in cooperation with all participating agencies such as CCG, CIRCL and CASES. A common and harmonised risk assessment approach is foreseen. Emphasis is placed on common understanding of the taxonomy of threats and the methods to evaluate impacts. On this basis, a common vocabulary is adopted, so that cooperation and especially coordination and rapid threat analysis is possible. Operators of critical infrastructures will be integrated in this process of risk assessment and risk mitigation.

CIRCL invites national telecommunication operators on regular basis to facilitate exchange of good practice knowledge and share incident response strategies. Also CASES promotes the usage of a common risk assessment process by promoting best practice in this area.

Due to the fact, that Professionals of the Financial Sector have to comply with the strict security rules elaborated by CSSF, they have to run risk assessments and also implement appropriate improvements to the infrastructures they use. Without these assessments, they would not be able to implement the obligatory business continuity planning.

¹³ See: http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies/stock-taking-report/at_download/fullReport

Relevant emerging NIS risks

The emerging NIS risks in Luxembourg¹⁴ are strongly linked to the risks identified in the surrounding countries.

The Luxembourg citizens are also using worldwide websites and networks (e.g. Facebook). As no national alternative site has gained widespread acceptance (compared to France, Germany), Luxembourg is exposed to the worldwide risks.

Resilience aspects

The CCG together with the CTIE regulates resilience within governmental networks. The Luxembourg government has implemented a high availability communication network and runs an alerting network that is capable of using different technologies to reach key personnel. Luxembourg also participates in a European R&D project to improve the current situation. Many actions have been undertaken to harmonize risk assessment and improve coordination and response strategies. This approach will improve communicative and reactive competences of the Luxembourg government and operators of critical infrastructures. A Luxembourg network resilience methodology is being drafted, but is not yet established. It is still in a start phase: at this moment no structured activities were defined or no national plan was set up.

In the private as well as in the governmental communication networks, high priority is given to redundancy of communication networks. The former national operator has highly redundant networks, and due to the creation of a highly competitive environment, redundancy should still be increased. Government has undertaken several measures in order to further improve the level of redundancy. Public authorities as well as private owners and operators of critical infrastructures will be expected to develop measures in order to improve their resilience particularly in relation to business continuity plans.

The national e-communications regulator ILR is mainly focused on market competition. However in the areas of mobile communication, every operator has to assure a minimum coverage. Every operator has to report quality indicators to the ILR. These indicators are used for measuring availability and coverage. Incidents have to be reported to the ILR. We notice here that all these specifications/ requirements are closely linked to the approval of the article 13a related to the "Telecom package".

Due to the very strict regulation of banking in Luxembourg, partial regulation of telecommunication networks can be attributed, at least indirectly, to the CSSF, the banking supervisory authority. Especially the obligation for banks and associated entities to comply with security standards quoted in the laws regulating the Professionals of the Banking Sector (PFS). The CSSF also publishes minimum requirements in the area of security. While these may not be considered as good practice, nevertheless, they are important as they impose a minimum standard.

The new law on National Protection aims to develop and implement measures which will improve levels of preparation, protection and response to any crisis situation. The government as such, advised by CONATEL and CONATIC, has the ability, in the case of a national crises or a catastrophe, to requisition, for a limited period and following the principle of proportionality, public networks.

¹⁴ See: http://www.enisa.europa.eu/act/res/policies/stock-taking-of-national-policies/stock-taking-report/at_download/fullReport

The National Protection Structure foresees no formal audits. Compliance is monitored through mechanisms used in the development and implementation of measures and business continuity plans, coupled with physical inspections. As regards audits of the governmental networks, both, the network of the central government and the network for the cities/villages, are closely monitored. If a governmental entity does not comply with the IT security measures or technical obligations its sub-network can be disconnected from the governmental backbone.

Each administration is connected to the governmental backbone through a firewall controlled by the operators of the governmental backbone (CTIE). A strict policy of partitioning the governmental network has been implemented. Crisis can be kept local by this strict policy.

Within the national CERT of Luxembourg – CIRCL – and within CCG and HCPN a repository of good practice on resilience is available. The repository is being updated regularly.

Privacy and trust

Status of implementation of the Data Protection Directive

The Data Protection Directive has been implemented by the amended law of 2 August 2002 on the protection of persons with regard to the processing of personal data (the "DPA"). The Law of 27 July 2007 has simplified and amended the DPA.

The competent national regulatory authority on this matter is the Commission Nationale pour la Protection des Données (the "CNPDP"). We haven't notice in 2010 any major update with regards to the implementation of the Data Protection Directive.

Information Security aspects in the local implementation of the Data Protection Directive

The data controller must comply with the general data security obligations. A description of these measures and of any subsequent major change must be communicated to the CNPDP at its request, within 15 days.

Enforcement and data protection breaches

The DPA does not contain any obligation to inform the CNPDP or data subjects of a security breach. However, in certain sectors, the data controller may be required to inform regulators of any breach (for example, in the financial sector).

The CNPDP has the power to investigate and is entitled to engage in legal proceedings in the interests of the DPA. The CNPDP will notify the legal authorities (State Prosecutor or President of the District Court) of any offences of which it is aware.

In addition, the CNPDP may make administrative disciplinary sanctions. Without prejudice to the criminal sanctions introduced by the DPA and the actions for damages governed by ordinary law, in the event that a processing operation violates the formalities provided for under the DPA being undertaken, any person is entitled to introduce an action for discontinuance of that processing in summary proceedings.

NIS awareness at the country level

Awareness actions related to NIS in general

Since February 2001, the **Action Plan eLuxembourg**, the transposition of the eEurope Action Plan is launched. Over 70 projects are organized around major challenges, such as the development of new technologies for education and research or the development of telecommunication infrastructure. In 2003, the first results were visible with several utilities being available online¹⁵ and the good progress of Luxembourg in the benchmarking project eGouvernement by the European Commission.

CASES, the national NIS awareness portal of the Ministry of the Economy and Foreign Trade, was able to reach a broad audience by partnering with different newspapers as well as radio and television. CASES also targets a large audience offering many publications about information security on its official portal, uses new communication channels like Twitter and Facebook and provides an alerting and warning system for critical security flaws.

In Mai/June 2010, an awareness campaign called "Old password?"¹⁶ was launched to encourage citizens to choose better passwords. In this campaign 50000 toothbrushes were distributed. The slogan was "Passwords are like toothbrushes, you should choose them well, change them regularly, not share them.

BEE SECURE – the Luxembourg node of the European Safer Internet Programme - coordinates the Luxembourg celebration of Safer Internet Day and as well as a variety of other campaigns. BEE SECURE is also the umbrella label for all governmental information security awareness initiatives including CASES.

The **BEE SECURE** initiative welcomes interested people at the annual **autumn fair**. Depending on the current major awareness campaign the visitors are informed about different topics ranging from general information to detailed instructions.

Awareness actions related to Information Safety for children

BEE SECURE organizes presentations at conferences and schools on a continuous basis. I.e. in schools, they provide a course on Internet Safety, dealing both with technical and behavioural aspects. These presentations are mandatory for all first year classes of secondary school and approximatively 35% of primary school classes attend voluntarily.

BEE SECURE also answers to requests from parent organisations and teachers to provide presentations and trainings. An annual "lessons learned" report on this awareness program in schools can be found on www.cases.lu.

We notice here that material is made available to the public on a regular basis.

Awareness actions related to Information Security for industries

Annually, the Hack.lu¹⁷ sets up a conference about computer security, privacy, information technology and its cultural/technical implication on society. The mission of Hack.lu is to make a bridge between different stakeholders (i.e. citizens, large organizations, government organizations) and the computer security world. The last hack camp held on October 2010.

¹⁵ See: <http://www.cases.lu>

¹⁶ See: http://www.cases.public.lu/fr/actualites/actualites/2009/01/25_orange/index.html

¹⁷ See: <http://www.hack.lu>

In October 2010 a special conference “Meet the hackers” was organized by the Ministry of the Economy and foreign Trade during which managers from the private sector and security specialists were brought together.

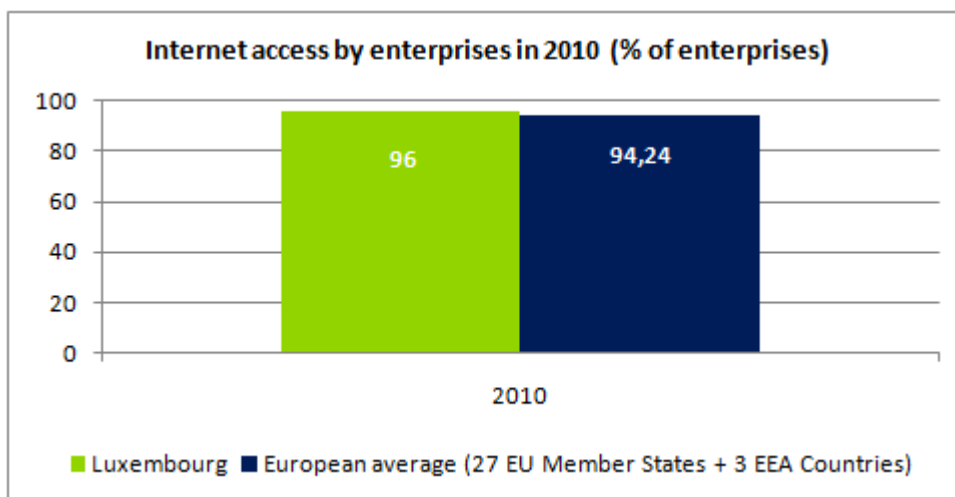
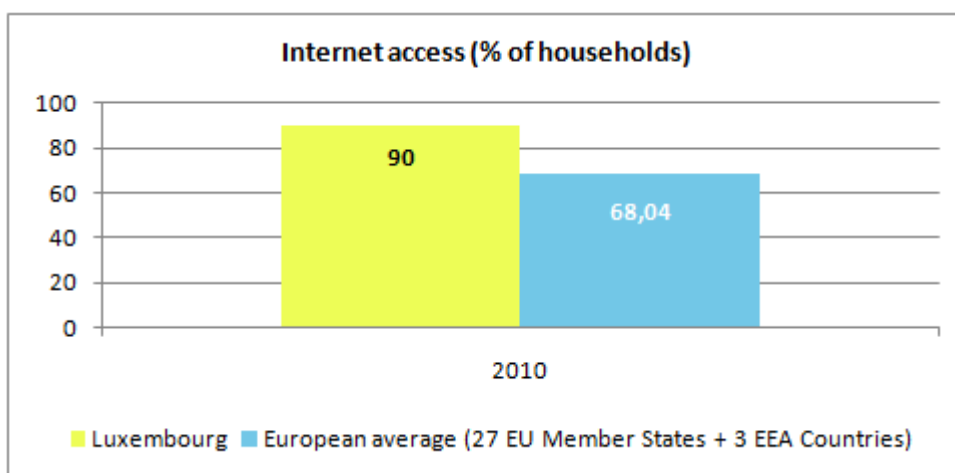
An information sharing platform has been established for the financial sector as well as Internet service providers. CASES also provides an information security policy to SMEs as well as governmental organizations.

Relevant statistics for the country

In order to provide the reader with additional information about the relative stage of NIS development in Luxembourg, a series of relevant statistics are included in this section. These statistics show that Luxembourg is above the European average in regards of Information Technology.

Internet access of population and enterprises

The following graphs, based on Eurostat information, provide an overview of the situation¹⁸ of Internet access in Luxembourg for enterprises and respectively households, relative to the European average.

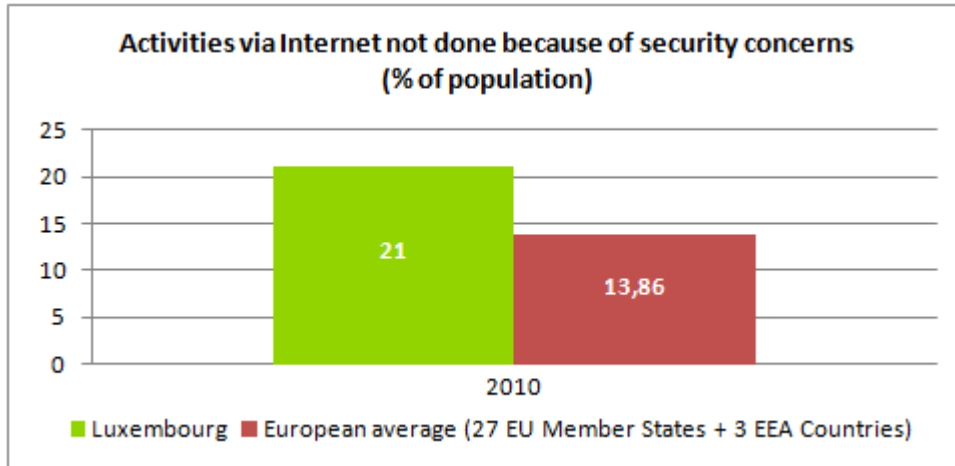


In 2010, the statistics indicate that both the enterprises and the households in Luxembourg have a level of Internet access that is above the European average.

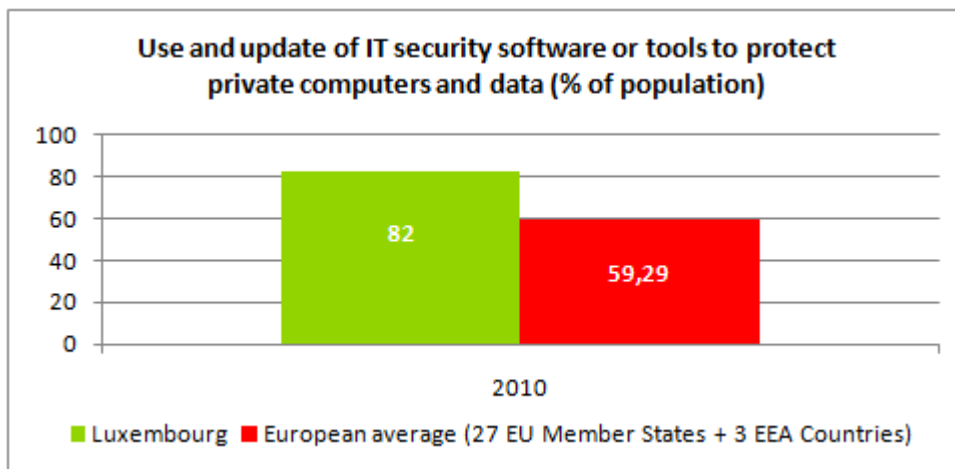
¹⁸ Source: Eurostat

Statistics on use of Internet by individuals and related security aspects

The percentage of population in Luxembourg that is reluctant in performing activities via Internet (e.g. e-banking, purchases of goods and services over Internet, etc.) because of security concerns is highly above the European average:



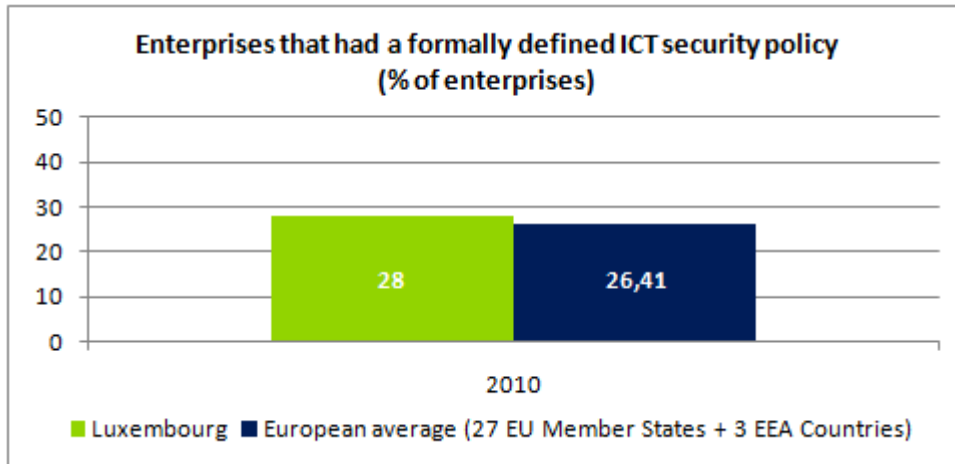
This can be an indication of either less confidence in web-based transactions or of more awareness of the general public regarding IT threats.



Also, it appears that the use of security tools to protect private computers and data is highly above the European average.

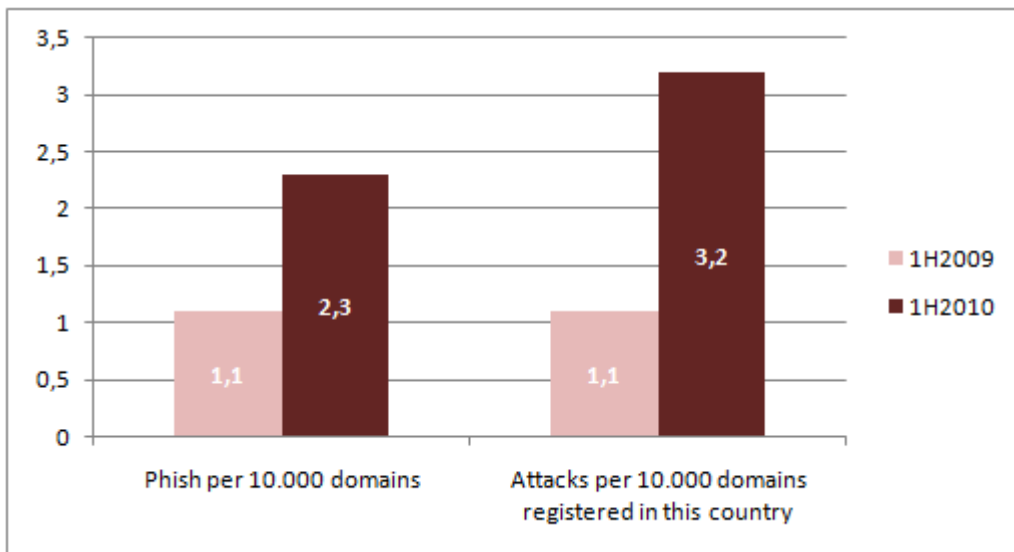
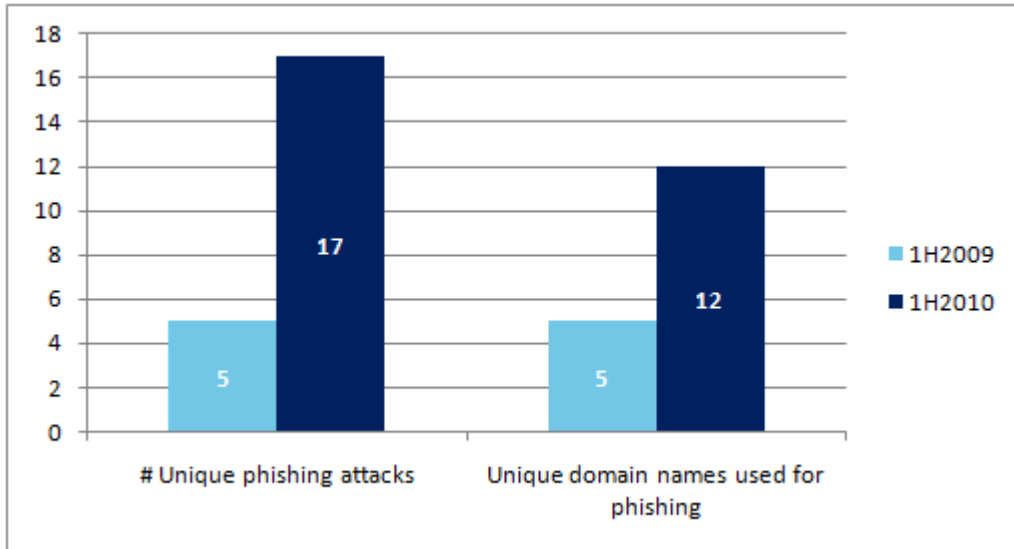
Statistics on use of Internet by enterprises and related security aspects

More enterprises in Luxembourg have a formally defined ICT security policy, compared with their European peers. See below:



Other Statistics

It is interesting to also mention that during the 1st half of 2010, and respectively for the 1st half of 2009, Luxembourg was mentioned in the global report¹⁹ published by the Anti-Phishing Working Group (APWG) with the following relevant statistics:



¹⁹ See: *Global Phishing Survey: Trends and Domain Name Use 1H2010*, available at: http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_1H2010.pdf

APPENDIX

National authorities in network and information security

National authorities	Role and responsibilities	Website
1. Direction of the electronic trade and information security in the Ministry of the Economy and Foreign Trade	This Direction of the ministry is in charge of the elaboration, update and implementation of the policy related to electronic trade, including amongst the legislation of the electronic signature.	www.eco.public.lu/attribution/dq3/d_communications/index.html
2. Cyberworld Awareness and Security Enhancement Structure (CASES)	CASES is the National Internet portal for information security. This structure is awaking awareness on systems and network security risks with a focus on Internet banking and Kids (Cases for Kids) using their website.	www.cases.public.lu
3. BEE SECURE	A common initiative between the Ministry of the Economy and foreign Trade, the Ministry of the Family and Integration and the Ministry of Education and Vocational Training. As awareness centre co-financed by the EU Safer Internet Programme, BEE SECURE raises awareness and informs the public about the safe use of the internet and new technologies. Its public is the Luxembourgish citizen of any age as well as communal and governmental institutions and private companies. BEE SECURE is also the umbrella label for all governmental information security awareness initiatives including CASES.	www.bee-secure.l
4. "Security made in Lëtzebuerg" (SMILE)	SMILE is a government financed "goupement d'intérêt économique - g.i.e." (economical interest group). It's missions are to support CASES and CIRCL in it's different tasks, like awareness raising, security policy and risk assessment promotion, incident handling and coordination. These services are provided to citizens, companies and local government entities.	www.smile.public.lu/
5. Commissionership of the national protection - Haut Commissariat a la Protection Nationale (HCPN)	On the international level, the HCPN acts as a national representative inside European Union, NATO and to any international organisation which is dealing with the crisis management and emergency plans. On the national level, the HCPN has three main roles: <ul style="list-style-type: none"> • Identification and analysing possible threats • Organising crisis centre for the CMPN if crisis occurs • Advice political authorities on security issues. 	www.hcpn.public.lu
6. Ministerial Council of the national protection - Conseil Ministériel de la Protection Nationale (CMPN)	CMNP is the decision-making body in charge of the crisis management. The CMPN members need to react quickly in order to analyse the imminent threat and provide advices to the CSPN (Conseil Supérieur de Protection Nationale).	www.hcpn.public.lu/protection_nationale/organisation/cmpn/index.html
7. National committee of telecommunications - Comité national des Télécommunications (CONATEL)	This comity is responsible for: <ul style="list-style-type: none"> • Establishing an inventory of telecommunication networks and services available and defining the needs for the national defence's reasons and the public security. • Organisation, coordination and preparation of 	www.hcpn.public.lu/comites_nationaux/conatel/index.html

National authorities	Role and responsibilities	Website
	<p>plans related to the use of telecommunication networks and services in exceptional case, such as the priority accesses to the public authorities' networks and the emergency services.</p> <ul style="list-style-type: none"> • Preparation of the plans for a quick recovery of the telecommunication networks and services in case of destruction or failure. • Insuring that the instructions for the plans' execution are communicated to the concerned parties and that these parties take the necessary measures for their missions' execution. • Organisation of periodically exercises. 	
8. National committee of critical infrastructure - Comité national de l'infrastructure critique (CONATIC)	<p>CONATIC establishes an inventory per category of all the national critical infrastructures and their dependences. Also, this comity sets the priority in function of the risk, determined by the infrastructure's value & vulnerability and the impacts and the consequences of the damages. The national protection concept of critical infrastructure is established by CONATIC. As key part in the critical infrastructure, the adequacy of the plans and procedures via simulations or exercises are checked by the CONATIC.</p>	<p>www.hcpn.public.lu/comites_nationaux/conatic/index.html</p>
9. Regulatory institution of the Luxembourg - Institut Luxembourgeois de Régulation (ILR)	<p>This independent regulatory body is responsible for the telecommunications, post, radio, electricity and gas sectors. The IRL regulates Electronic communications and issues annual report regarding the current situation of telecommunications, post radio, electricity and gas sectors.</p>	<p>www.ilr.etat.lu</p>
10. Centre of Technologies and information for the national government - Centre des Technologies de l'Information de l'Etat (CTIE)	<p>CTIE is a government IT department responsible for e-governance and administrative simplifications. Its main tasks are to:</p> <ul style="list-style-type: none"> • Plan, coordinate and assist IT services for the national government. • Produce and customise secure administrative documents • Standardize government websites (homogeneous look) 	<p>www.ctie.public.lu</p>
11. National commission of the data protection - Commission National pour la Protection de Données (CNPD)	<p>CNPD is a national body for data protection and privacy issues. Its duties are to ensure compliance with legislation and the regulatory framework on personal data, and to provide input to the government on laws and measures in the area of the creation and processing of personal data.</p>	<p>www.cnpd.lu</p>
12. Communication centre of the government -Centre de communication du gouvernement (CGC)	<p>CCG is a governmental body for security of telecommunication and IT. It advises administration in telecommunication, IT and security. The missions of the CGC are to:</p> <ul style="list-style-type: none"> • Advice the government administration in the telecommunications, the encrypted information and the security. • Insure the function of security authority for the telecommunication and IT systems. • Insure the function of Certification authority for communication systems with a public key infrastructure • Represent the government close to International organizations in the telecommunications, the encrypted information and the security areas. 	<p>www.ccg.public.lu</p>

National authorities	Role and responsibilities	Website
13. Service of media and communication - Service des Medias et de la Communication (SMC)	<ul style="list-style-type: none"> • Make available to the government and the main national administrations the specific means of telecommunications and IT. • Be the crisis centre for the government. <p>The portal of the SMC publishes all the national policies in the area of Telecommunication, such as electronic communications, electronic trade and electronic signature. The SMC encourages investments in media and information technologies.</p>	www.mediacom.public.lu
14. National regulator for the financial sector - Commission de surveillance du Secteur Financier (CSSF)	<p>The CSSF ensures that the laws and regulations governing the various areas of the financial sector are enforced and observed.</p> <p>It issues Circulars complementary the regulatory framework. Through these Circulars, the CSSF clarifies the implementation modes of different legal provisions governing the supervised entities, publishes prudential rules relating to specific activities and gives recommendations regarding financial activities.</p>	www.cssf.lu
15. National Education and Research Network - Réseau Téléinformatique de l'Education Nationale et de la Recherche (RESTENA)	<p>High speed network for the education and research community of the Grand Duchy of Luxembourg, RESTENA aims to provide network services for all public and private institutions and organizations involved in the field of education, research, culture, health and administration. RESTENA operates the RESTENA CSIRT that offers support and coordinates security incident response within its community. The CSIRT also serves as a trusted point of contact and acts as clearing house for security incident-related information, and works to improve awareness and knowledge of IT security among the community's members. RESTENA CSIRT keeps contact with other CSIRT/ CERT teams and cooperates with national and international CERT organizations.</p>	www.restena.lu
16. Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services (ILNAS)	<p>The Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services (ILNAS) is a public service under the authority of the Minister in charge of the Economy.</p> <p>For complementarity, efficiency and transparency reasons and for the purposes of administrative simplification, ILNAS brings together under a single entity several administrative and technical activities which used to come under the authority of several public entities, such as standardization, accreditation, audits of laboratory good practices, market surveillance of electric and telecommunication equipment, toy safety and general product safety, digital trust, quality promotion, legal metrology and the designation of notified organizations according to the "New Approach" directives.</p> <p>The Digital Trust Department of ILNAS is responsible for the accreditation and supervision of Certification Service Providers, and for the implementation and management of Luxembourg "Trusted List of supervised/accredited Certification Service Providers" providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by Luxembourg for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament</p>	www.ilnas.public.lu

National authorities	Role and responsibilities	Website
	and of the Council of 13 December 1999 on a Community framework for electronic signatures. The Digital Trust Department promotes the excellence of Information technology by the application of high level quality and security tools, and the well-understanding and awareness of the standardization in this field. The Digital Trust Department of ILNAS will plan in 2011 a specific "National ISO/IEC/JTC1 Day", with some focuses on information security aspects.	
17. Consumer Association of Luxembourg - Union Luxembourgeoise des Consommateurs (ULC)	A consumer organization, its aim is to protect, defense, inform and educate consumers in Luxembourg. UCL represents the consumers nearby the political and public institutions.	www.ulc.lu
18. Centre Européen des consommateurs (CEC)	<p>The European Consumer Centre Luxembourg (ECC Luxembourg) GIE is part of a network of 29 ECCs in the European Union plus Iceland and Norway (ECC-Net).</p> <p>The ECC Luxembourg was created in 1991 under the name "Euroguichet" and celebrates its 20th anniversary in 2011. Since 2003, the ECC operates as the "Economic Interest Group (GIE). The ECC Luxembourg is financially supported by the European Commission, the Luxembourg government (Ministry of Economy and Foreign Trade) and the Luxembourg Union of Consumers (ULC). ECCs fulfill primarily the following tasks:</p> <ul style="list-style-type: none"> • Inform the consumer about the European consumer law and European policy in the field of consumer issues. • Advise consumers in cross border disputes. • Assist consumers in their cross border disputes with a company registered in another EU country. 	www.cecluxembourg.lu/

Computer Emergency Response Teams (CERTs)

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> • FIRST²⁰ member • TI²¹ listed 	
19. CIRCL	<p>CIRCL is the Computer Incident Response Centre Luxembourg of Governmental administrations and ministries of the Grand-Duchy of Luxembourg. Its missions are:</p> <ul style="list-style-type: none"> • Provide a systematic response facility to ICT-incidents • Support to the constituency recovering quickly and efficiently from security incidents and minimise loss or theft of information and disruption of services • Gather information during incident handling to better prepare for handling future incidents and to provide better protection for systems and data • Provide an security related alerting and 	www.circl.lu

²⁰ See: <http://www.first.org/members/teams/>

²¹ See: <http://www.trusted-introducer.nl>

CERT	Role and responsibilities	Website
	<ul style="list-style-type: none"> • FIRST²⁰ member • TI²¹ listed <p>warning system for its constituency's ICT-systems</p> <ul style="list-style-type: none"> • Foster a knowledge exchange within the constituency. <p>We notice here that CIRCL is:</p> <ul style="list-style-type: none"> • Not First member; • TI listed. 	
20. RESTENA-CSIRT	<p>RESTENA-CSIRT is the Computer Security Incident Response Team of RESTENA, the high speed network for the education and research community of the Grand Duchy of Luxembourg. The mission and goals are to:</p> <ul style="list-style-type: none"> • Support and coordinate security incident response within the constituency; • Serve as a trusted point of contact and act as clearing house for security incident-related information; • Improve awareness and knowledge of IT security among the constituents; • Keep contact with other CSIRT/ CERT teams and cooperate with national and international CERT organisations; <p>RESTENA-CSIRT's constituency is the user community served by RESTENA Foundation. This includes:</p> <ul style="list-style-type: none"> • University of Luxembourg; • Higher education institutions; • Public and private research centers; • Cultural institutions; • Primary and secondary schools; • Individual users of RESTENA services. <p>RESTENA-CSIRT is not First member; but it is TI listed.</p>	www.restena.lu/csirt
21. ASBL CSRRT-LU	<p>ASBL CSRRT-LU is a computer security research and response team association localized in the Grand-Duchy of Luxembourg. ASBL CSRRT-LU engages in highly advanced computer security development and research projects in order to increase security awareness and advancement especially in Luxembourg but also on an international level. ASBL CSRRT-LU is in close partnership with research institutes, the industrial sector and governmental institutions. CSRRT-LU provides a cooperative and virtual organization for working with individuals, groups and industries.</p> <p>ASBL CSRRT-LU is not First member & not TI listed.</p>	www.csrst.org

Industry organisations active in network and information security

Industry Organisations	Role and responsibilities	Website
22. Internet Society in Luxembourg (ISOC)	<p>ISOC - a non-profit organization - was created to coordinate and follow-up the Internet in Luxembourg and in the Saar-Lor-Lux area. The key areas of activity of the ISPA include:</p> <ul style="list-style-type: none"> • Offering a forum for discussions related to the standards, security, laws, economy, communication, ... • Lobbying nearby the telecommunication operators and the regulation authorities to obtain the lower rates; • Promoting the diversity of languages on the Internet. 	www.isoc.lu
23. Professional association of Information Security - Association des Professionnels de la Société de l'Information (APSI)	<p>The Association for Professionals in the Information Society (APSI) is a non-profit business association of professionals working in the field of information. The SIPA aims to promote the creation of public and private initiatives in the areas of information society in the Grand Duchy of Luxembourg. They organise working groups around NIS topics.</p>	www.apsi.lu
24. Fedil - Business Federation Luxembourg	<p>FEDIL - Business Federation Luxembourg is a federation of companies representing different sectors of industry, construction and business services. The Federation carries a mission of information, assistance and advice to its members. One of the five working groups composed of experts selected from within the member companies, examines and prepares the decisions taken by the Board on the theme of Information Technology and Communication (ICT), covering in particular:</p> <ul style="list-style-type: none"> • Telecommunications infrastructure; • eLuxembourg; • eAdministration; • Computers; • Innovation. 	www.fedil.lu/accueil
25. CLUSIL	<p>CLUSIL is a non-profit association of experts in the fields of information security. CLUSIL contributes to information security education, improvements, and awareness via publications resulting from the activity of its work groups, market studies, and public conferences. Most of the documents resulting from these activities are made publicly available. CLUSIF also regularly initiates public studies on cyber-crime and security policies. An important contribution of CLUSIL to the management of information-related security is a comprehensive risk management methodology, called MEHARI, which is built around a set of modules, tools, and questionnaires.</p>	www.clusil.lu/tiki-page.php?pageName=Mission

Academic organisations active in network and information security bodies

Academic Organisations	Role and responsibilities	Website
26. Laboratory of Algorithmic, Cryptology and Security (LACS) (at the University of Luxembourg)	LACS is part of the Computer Science and Communication Research Unit. The LACS researches are relevant to the financial place of Luxembourg or the emergence of the e-government in Luxembourg relying on confidential and trusted communications.	www.uni.lu/recherche/fstc/laboratory_of_algorithmics_cryptology_and_security
27. Interdisciplinary Centre for Security, Reliability and Trust (at the University of Luxembourg)	This national Centre creates a European centre of excellence and innovation for secure, reliable, and trustworthy ICT systems and services. A platform for research collaboration with national and international partners is provided, and for participation in national and international funding programs. This Centre establishes a high quality and internationally attractive PhD program. This objective is to create a positive impact on the regions financial, content/services, and communication/networking sectors. Furthermore, the Centre permits to make available a meeting place in Luxembourg for knowledge transfer and exchange of ideas with a special focus on small and medium sized businesses. It permits to foster efficient dissemination of research results commercially as well as academically.	www.securityandtrust.lu
28. Public Research Centre Henri Tudor	Public Research Centre Henri Tudor is a Luxembourg-based research institute. It has for main mission to contribute to the improvement and the strengthening of the innovation capacities of enterprises and public organizations. The Public Research Centre Henri Tudor's activities are oriented towards five scientific and technological fields, including Information and Communication Technologies (ICT). The ICT department at the Public Research Centre Henri Tudor aims to cooperate inside the economy via the Researches and the innovation's advices towards the promising ICT applications.	
29. Public Research Centre Gabriel Lippmann	This public establishment is devoted to applied scientific research and technological development, as well as permanent technology transfer and high-level training. Founded in 1988 to give commercial companies and the public sector in Luxembourg a scientific partner that is skilled in computer science, ISC (Informatique, Systèmes et Collaboration) now has much experience of collaboration with the Luxembourgian world. ISC is specialized in the following four main fields of research: <ul style="list-style-type: none"> • Information system modeling • Information system architectures • Software engineering • Language engineering Moreover, the Computer Supported Cooperative Work (CSCW), the IT and organisational aspects of e-business and e-government, the Human-Computer Interaction (HCI) and visualization techniques and the IT security are covered by the Centre.	www.crpq.lu

Other bodies and organisations active in network and information security

Others	Role and responsibilities	Website
30. ISACA LU	ISACA is a Worldwide association of IS professionals dedicated to the knowledge and good practices regarding audit, control, and security of information systems. The chapter in the Luxembourg organizes local events such as education and training, workshops, roundtables and other specific events.	www.isaca.lu/
31. OWASP – Luxembourg local chapter	The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. The main objectives of OWASP Luxembourg Local Chapter is to educate and create awareness amongst the industry, developers, project architect, security officers on the security issues of web applications.	www.owasp.org/index.php/Prague
32. Syn2cat	The typical activities of Syn2cat include <ul style="list-style-type: none"> • Learning and sharing knowledge; • Presentations and lectures; • Social activities including games and parties. 	www.hackerspace.lu/
33. Luxtrust	LuxTrust is a certification authority established between the Luxembourg government and major private sector actors of Luxembourg, in particular the financial sector.	www.luxtrust.lu

References

- ENISA, Information security awareness in financial organisation, November 2008, available at http://www.enisa.europa.eu/doc/pdf/deliverables/is_awareness_financial_organisations.pdf
- An overview of the eGovernment and eInclusion situation in Europe, available at: <http://www.epractice.eu/en/factsheets>
- CIRCA-FI: http://www.enisa.europa.eu/cert_inventory/pages/04_01.htm#02



PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu