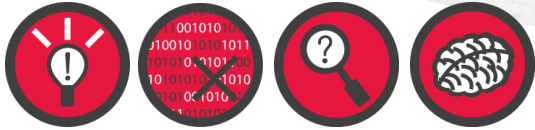




itrust
consulting



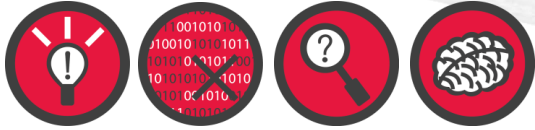
Tailoring information security to
business requirements

10-year anniversary

itrust consulting s.à r.l.
Z.I. Bombicht
L-6947 Niederanven

Tel: +352 26 176 212 6
Fax: +352 26 710 978
Web: www.itrust.lu

Dr. Carlo Harpes
Founder and
Managing Director



1. History

Thanks to the enablers:



1. History

The first year

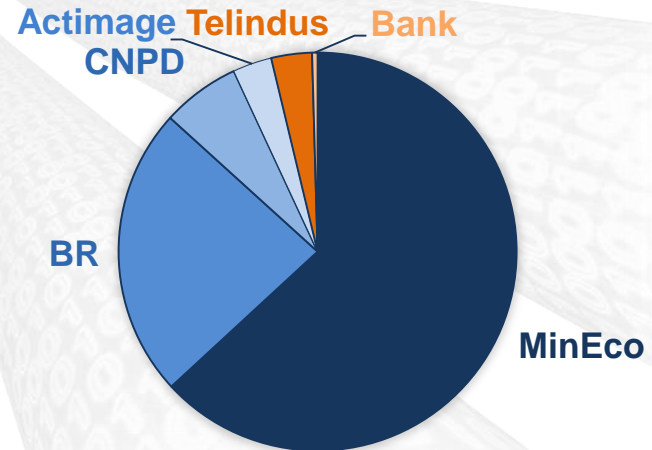


- **itrust**: acronym of

“Information:

Techniques and Research for Ubiquitous Security and Trust”

- An SME from Luxembourg specialising in Information Security Systems
- Created Jan 4th, 2007
- First recruitment, myself, on March 1st, 2007
- First customers:



1. History

The first growth

- First location: my home
- First students: Feb 2008: 2 BACH-UL, March-Aug: 2xMSSI-Metz
- First recruitments: June 2008
- First office building: Ecostart in Foetz
- First research projects:
 - Sept 2008: MICIE
 - Oct 2008: Bugyo beyond
- First service portfolio:



1. History

Learning to fly

- Auditing ISO 27001 for SNCH (2008)
- Developing new Business lines
- Engineering products:
 - APSARA (2010), TRICK tester (2013), TRICK light
 - Introduction of SCRUM for Software development
- Going to space:
 - Study, then proof-of-concept for secure Galileo localisation
- Working for European institutions:
 - CURIA Audit in 2008
 - Pentesting
 - Staffing (since: 2011)
- Preparing certifications (Euroscript, LuxCloud...)
- Moving to Niederaanven (2012)



1. History

R&D projects



On-going projects

H2020 - ATENA: Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures

H2020 - bloTope: Building an IoT OPen innovation Ecosystem for connected smart objects

MinEco - SmartGrid Luxembourg Cockpit: Real-time risk monitoring tool for critical infra.

FNR - IDS₄ICS PhD on Intrusion Detection Sys. and Risk monitoring for Industrial Control Sys.



ATENA



Former projects

FP7 - CockpitCI: Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures

FP7 - TREsPASS: Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security

ITEA2 - DIAMONDS: Security Testing Tool development

ESA - LASP: Localisation Assurance Service Provider (POC)

FP7 - Liveline: Live ICT services Verified by EGNOS to find Lost Individuals in Emergency situations

FP7 - MICIE: Design of a risk prediction tool for interdependent Critical Infrastructures

CELTIC - BUGYO Beyond: Building security assurance in open infrastructure beyond

CIPS - SPARC: Space Awareness for Critical Infrastructures

FP7 - i-Going: i-Galileo indoor navigation (Galileo signal i-enabled by pseudolites for indoor navigation)



1. History > Important events

Cybersecurity attack on APT-1

- Counterstrike by Hacker of itrust consulting against APT-1
- Technical report released with logo of itrust consulting
- Alerting of authorities 3 months before
- Discussion of legal constraints on cybersecurity in the U.S.
- No media coverage in LU
- Shift of activity/Customer

Luxembourg: The Steve McQueen of Cybersecurity Pourquoi?

- Article du 12 avril sur internet, par Stewart Baker, ancien « first Assistant Secretary » du US Department of Homeland Security sous George W. Bush
- Il publie une **interprétation politique** d'un article technique de Paul Rascagnerès, itrust consulting, du 8 avril 2013.

Stewart Baker conclut:

- "Now we owe a lot to Paul Rascagnères, though he seems to have treated the Justice Department's line the way Steve McQueen treated the fence in The Great Escape.
- Well, God bless him, he's showing us a new path to cybersecurity."



itrust
consulting

Type Public document
Project APT1: technical backstage
Title malware analysis
Classification Public

6 Conclusion

In this report, we document how we could reveal the methodology and tools used by an attacker. The used technologies were commonly known, which supports our fears that such kind of APT affects more and more infrastructures. Among them we can find public companies, governmental and political institutions... The most efficient and proactive way to protect an infrastructure and fight back the attackers is to understand their attacks and the way they work. An interesting fact is to see the professionalization in this field. Here are some key facts about the attackers:

- More than 300 servers
- Use of proxy servers to hide their activities;
- one server per target;
- custom made malware
- working hours, such as office employees
- really good organization
- ...

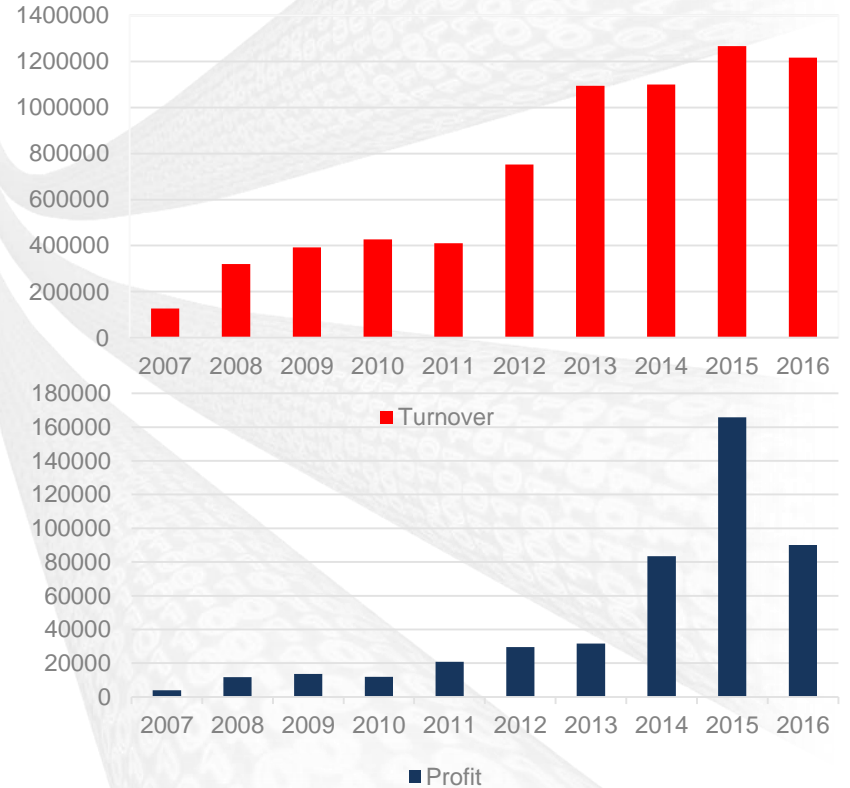
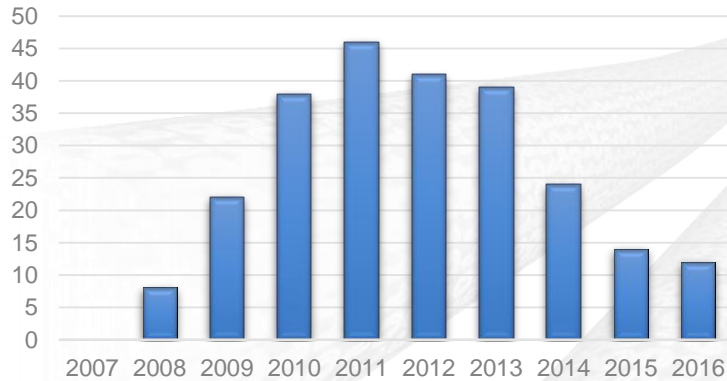
Infrastructures such as the one detailed in this report are expensive but Intelligence is a real issue. People or organisations seem do not hesitate to pay for such illegal information theft.

"The only real defense is offensive defense" (Mao Zedong)

1. History

A success story

% RD





2. Out-of-the-Box Thinking

2. Out-of-the-Box Thinking

2.1. Since 2007

Tailoring information security to business requirements

- Security has to support the added value process,
- No documents, no risk assessment methodology fits all organisations, all cultures,
- Security is more a process, not a final state.

2. Out-of-the-Box Thinking

2.1. Since 2007

Combining R&D and Consulting

itrust consulting a mix of:

- the first research institution without base funding,
- a big-4-like consulting organisation,
- a technology-driven engineering company,

reduced to the size of a small company.

2. Out-of-the-Box Thinking

2.1. Since 2007

Interdisciplinarity beats competition

itrust consulting hired a team of very different experts that:

1. each have their own area of expertise,
2. are willing to work in a team,
3. work according to a common, but flexible methodology,
4. aim to create value for our customers,

No common job description,

Staff from 11 different nationalities



2. Out-of-the-Box Thinking

2.2. Four new principles

1. On Trust

Be certified before your customers ask it of you!

- Certification is the foundation of trust
- Be proactive, demonstrate that you know your customers' needs before they do.

itrust consulting has just been certified ISO-27001

- We do what we ask of our customers.
- We demonstrate that this is feasible, even for a small organization, without requiring heavy, high-tech investment.



2. Out-of-the-Box Thinking

2.2. Four new principles

2. On Efficiency

Run a single management system!

- Most organisations have a silo management approach for managing their business
- Creating conflicts for influence, and inefficiencies
- ISO 27001 is the first management standard we implemented that replaced PDCA with a better structure:
- Extend this ISMS to cover other domains.



2. Out-of-the-Box Thinking

2.2. Four new principles

3. On Effectiveness

Be prepared for disruptive changes!

The facts:

- 1. Technological changes create new actors:** No horse equipment company built cars, Microsoft rose because computer manufactures did not build OS, ...
- 2. Political systems change fast:**
 - France took only one year to give an absolute majority to an unknown party,
 - US to lose reliability (the character of a single person has more influence than that decades of foreign policies).
- 3. Political acceptance of technological changes:**
 - Merkel decides spontaneously to stop nuclear power plants as a reaction to Fukushima.

The questions:

- Are existing banks able to manage Fintech?
- Are existing car manufacturers struggling with CO2 scandals able to dominate the eCar and autonomous driving market?
- Are current social network operators the leaders in the IoT?

2. Out-of-the-Box Thinking

2.2. Four new principles

4. On Flexibility

You don't decide!

- Be humble!
 - The market decides.
 - Your customer decides.

You have to adapt your service to the interested parties.

- Cybercrime will grow, spying will be omnipresent.

You can only help your customer to be prepared and provide reliable guidance.



3. Our services and solutions

Integrated ISMS

Information Security Management System



Information Security Management System (ISMS)

General policy (ITR-General)

Information Security Management System (ISMS)

Information Security Policy

General information	
Reference number	0-0
Version	1.0
State	Final version
Approved by	CMC
Approval date	23/02/2015
Classification	Internal

Informations générales

Número de séquence	15-0
Etat	Final
Classification	Interne

Relation avec les fo

Système de Gestion de la Sécurité de l'Information (SGSI)

Gestion des risques

Information générale

Número de séquence	05-00
Sub-ide	Version : 1.0
documentación	Etat : Approuvé
Approuvé par	Philippe Mathieu
Date d'approbation	04/03/2019
Classification	Restreinte

Politique de Sécurité de l'Information de l'Etat luxembourgeois

Politique générale (PSI-LU)

Informations générales

Número de séquence	0-0
Version	1.0
Etat	Version finale
Propriétaire	ANSSI
Classification	Vert

General Information

Type	Policy
Sequence number	000
Version	3.1
State	Final
Approved by	C. Herpes
Date	04/03/2019
Classification	Internal

The currently applicable version of this document is on drive D:\...

But du document
Cette politique sectorielle définit les directives relatives appliquées et respectées pour protéger de manière adé les informations du Centre des technologies de l'informa

Avant-propos du Premier Ministre, Ministre d'Etat
La protection des informations est une priorité majeure pour le gouvernement du Grand-Duché de Luxembourg, et nécessite une politique dédiée à la sécurité de l'information. Elle concerne la confidentialité, l'intégrité et la disponibilité des informations gérées dans les systèmes d'information classifiés et non classifiés installés et exploités par l'Etat et les opérateurs d'infrastructures critiques pour leurs besoins propres.

La formulation de cette politique permet de mettre en œuvre la stratégie de cybersécurité approuvée et rendue exécutoire par le Conseil de gouvernement. Elle constitue l'outil principal de la gouvernance de la sécurité des informations internes à l'Etat et prépare le développement de la sécurité numérique dans l'esprit de l'initiative « Digital Letzebuerg ».

Cette politique énonce des objectifs généraux et définit un cadre de gestion d'objectifs, spécifiques par domaine et par entité. La mise en application de cette politique crée un Système de Management de la Sécurité de l'Information (SMSI) pour les départements ministériels, les administrations et services de l'Etat luxembourgeois, ainsi que pour les opérateurs d'infrastructures critiques. Ce SMSI définit, met en œuvre, surveille et améliore des objectifs de sécurité, ainsi que des actions et consignes appropriées pour répondre à ces exigences.

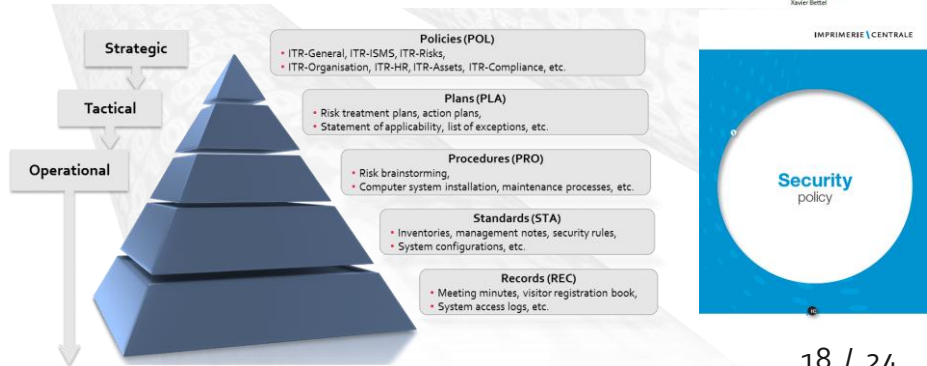
La gouvernance de la sécurité s'articule autour de dix principes élaborés par l'ANSSI, dont voici trois éléments clés :

- Afin d'atteindre les objectifs énoncés et de minimiser les risques liés aux traitements des données, la sécurité de l'information, incluant la sécurité des systèmes d'information, s'exerce au cœur de toutes les activités de l'Etat luxembourgeois.
- Le système de gestion prévoit que les départements ministériels, les administrations et services de l'Etat luxembourgeois établissent des mesures appropriées de protection de l'information contre toute modification, destruction et divulgation non autorisée, quelle soit accidentelle ou intentionnelle. Le cas échéant il protège aussi la fiabilité et la non-répudiation de ces mêmes informations. Il recourt à une analyse des objectifs et à une analyse des risques.
- Ce document, ainsi que toutes exigences énoncées dans ce cadre et tout document annexé ont un caractère obligatoire pour tout le personnel des leur publication par l'ANSSI et leur mise en application par le dirigeant des départements ministériels, administrations et services de l'Etat luxembourgeois concernés.

Je vous invite à prendre connaissance de l'engagement demandé à chaque agent, et à contribuer avec toutes vos compétences à la réalisation de l'objectif ultime qui est la protection adéquate des informations que vous devez traiter en vue d'assurer la confiance des citoyens, des entreprises exerçant une activité au Luxembourg, et des Etats partenaires dans les services de l'Etat luxembourgeois.

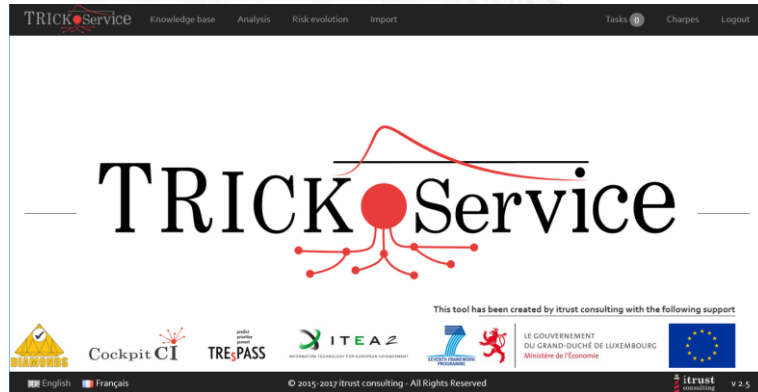
Xavier Bettel

- We write your documents.
- We consult you to improve your management.
- We deliver you a set of 27001 compliant policies and procedures tailored to your needs.

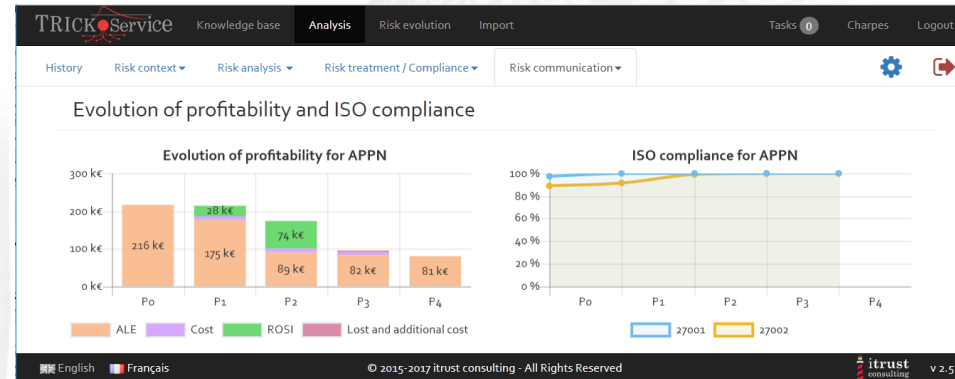


TRICK Service

Tool for Risk management of an ISMS based on a Central Knowledge base



1. Context & assets valuation (cf.2 7005, 29134)
2. Gap analysis (27002, 29151, 27552...;
3. Qualitatively assess threats, vulnerabilities, risks;
4. Quantified assessment of impacts and likelihoods;
5. Risk treatment plan, sorted by phases and ROSI;
6. DPIA compliant to GDPR, RAR compliant to CSSF.



SECurity as a Service (SECaaS)

A security fit for you

A swiss knife for your security

A customised service to implement a monitoring service adapted to the needs and budget of your company, by realising specific security sourcing missions. itrust provides mentoring or technical implementation missions on a one-off or regular basis onsite at your organisation.

Pool of competencies related to security

For a SME, implementing, maintaining and improving the security level of its organisation is a hard job: lack of time, lack of competencies or methodologies.

It is better to base your effort on a security team already trained rather to get the entire security work in addition to the core business.

Total flexibility

- Onsite or remotely
- Adapted to customers' responsibility org-chart and to their type of management
- itrust expertise resource as an internal service for you
- Control of cost and budget for defined objectives



CERT: Computer Emergency Response Team

- Incident Response
- Forensic Investigation
- Malware Analysis
- R&D
- Participation to international conferences (Defcon Las Vegas, hack.lu)
- Knowledge transfer (APT1: technical backstage)



itrust consulting CERT respects the incident-handling guidelines provided by NIST:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow-up

What we learned operating a CERT

- a lot on threats and malware,
- that in the future, all organisations SHALL manage how to react to security incidents, i.e., have CERTs as partners / subcontractors.

Ethical Hacking

- Penetration tests
- Vulnerability Assessment
- External Vulnerability Scans



TF-CSIRT
Trusted Introducer



Pseudonymisation

- EPSTANTTP, high data protection when assessing the quality of our schools

Security design for the Internet of Things

- Lightweight cryptography solutions
- Privacy-protecting policies
- Pseudonymisation

Critical infrastructure protection

- From TRICK Service to TRICK Cockpit (Risk Monitoring)
- ICS SCADA
- Vulnerability Management System
- Multi-antivirus platform AVCaesar

Conclusion

Our new slogan



To summarise our ideas in a single way, we complement:

Tailoring information security to business requirements

with



Move securely within the cyberworld

Thank you for your attention