Tailoring information security to business requirements

Research & Innovation on Security - Lessons learned

08/06/2015

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

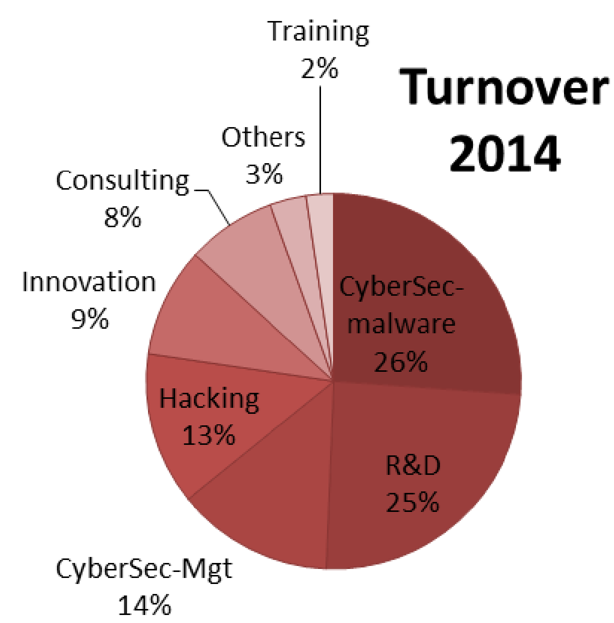
Tel: +352 26 176 212
Fax: +352 26 710 978
Web: www.itrust.lu

Dr. Carlo Harpes

itrust consulting s. à r. l.

Tailoring information security to business requirements

- itrust : acronym of “Information: Techniques and Research for Ubiquitous Security and Trust”
- An SME from Luxembourg specialising in Information Security Systems.
- Start-up of the year 2008
- Current staff 17 persons
- Turnover 2013 or 2014 : 1,1 M€



malware.lu CERT

itrust consulting operates CSIRT Services

CERT: Computer Emergency Response Team

- Incident Response
- Forensic Investigation
- Malware Analysis
- R&D
- Participation to international conferences
- Knowledge transfer, like on 27/3/2013 P. Rascagneres, APT1: technical backstage

Leassons Learned by operating a CERT:

- We learn a lot on threats and malware.
- Nobody is ready to pay for, except very large (governemental) organisations
- In future: all organistions SHALL manage how to react to security incidents, i.e. have CERTs as partners / subcontractors.

Pentesting

Hacking as a Service

Pentest activities:

- Vulnerability Scans
- Redteam pentesting
- Vulnerability assessments
- Technical audits

Leassons Learned:

- SME unaware of current risks.
- Missing care on security maintainance
- Missing appropriate Security Management Systems

Information Security Management Consulting

Security consulting activities:

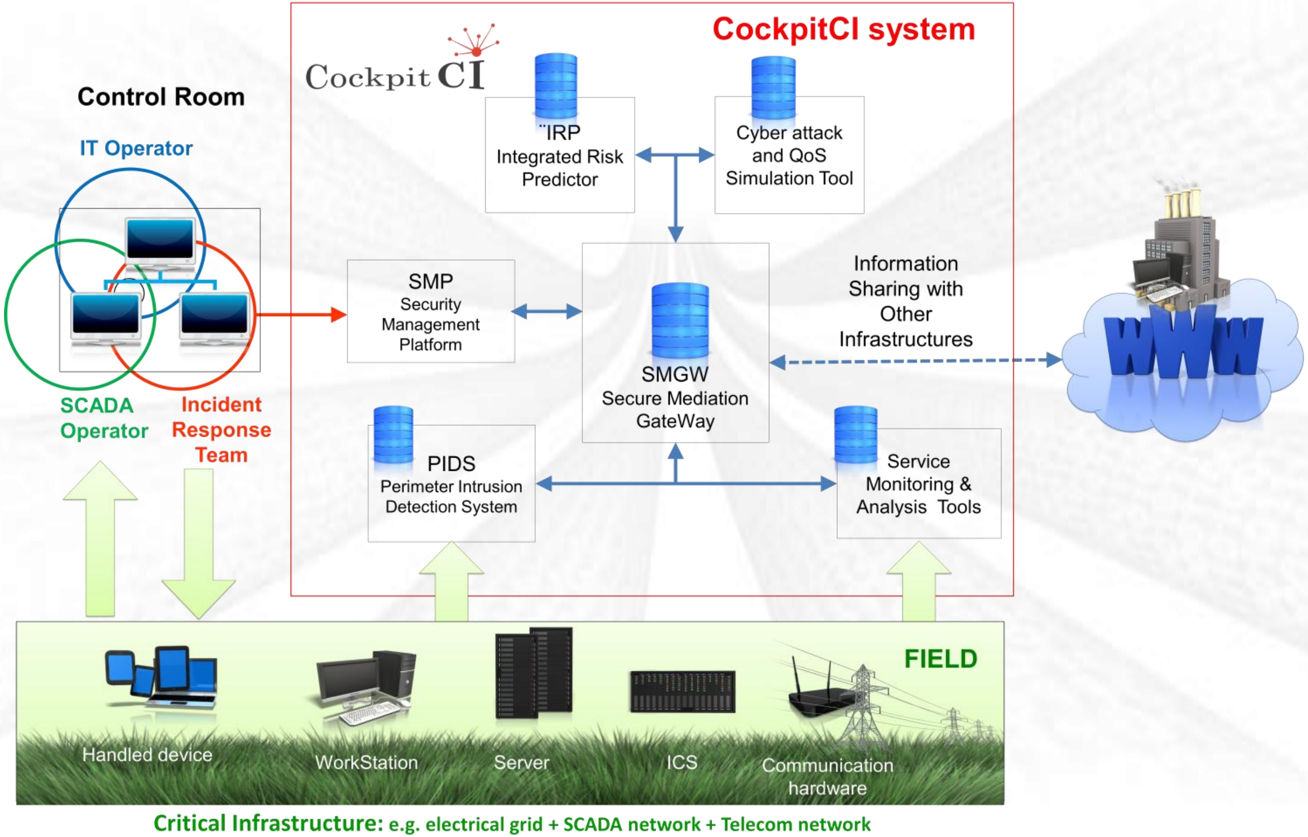
- ISO 27001 (ISMS) Implementation
- Risk assessment, i.e. with TRICK Service, a Web Service tool to assess and treat risk, developped by us in different R&D projects.

Leassons Learned :

- Increased demande for formal Risk Assessments and Risk Management
- Not enough customer ask for security, i.e., insufficient deployment of security certification
- Need for effective security management
- Need for more communication and knowledge on cybersecurity
- Need for online risk monitoring
- Need for better tools, which are fully exploited...

FP-7 CockpitCI

Cybersecurity monitoring



CockpitCI system

Cockpit CI

Control Room

IT Operator

SCADA Operator

Incident Response Team

¨IRP Integrated Risk Predictor

Cyber attack and QoS Simulation Tool

SMP Security Management Platform

SMGW Secure Mediation GateWay

Information Sharing with Other Infrastructures

PIDS Perimeter Intrusion Detection System

Service Monitoring & Analysis Tools

FIELD

Handled device

WorkStation

Server

ICS

Communication hardware

Critical Infrastructure: e.g. electrical grid + SCADA network + Telecom network

R&D background

On-going projects

FP7 TREsPASS (Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security): we lead development and integration of the TREsPASS tool, such as Attack Tree tools, TRICK Service, ...

SGLC (SmartGrid Luxembourg- Cockpit)…
We will create a real-time risk monitoring tool for the Lu smartmeter network and similar ICS.

Former projects

FP7 CockpitCI (Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures): CockpitCI defines and implements an online distributed risk predictor, and design a tool able to detect critical situations such as cyber attacks and enable reaction strategies.

DIAMONDS (Security testing): we developed malwasm, malware.lu CERT, ..

ESA project LASP (Localisation Assurance Service Provider): The LASP project, lead by itrust consulting, aims at developing a demonstrator to ensure the location correctness (subcontr. uni.lu).

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: we developped TRICK light.

CIPS SPARC (Space Awareness for Critical Infrastructures): with telespatio, Uni. Roma3…
The project will analyse the space threats, their impact and set up security good practices guidelines.

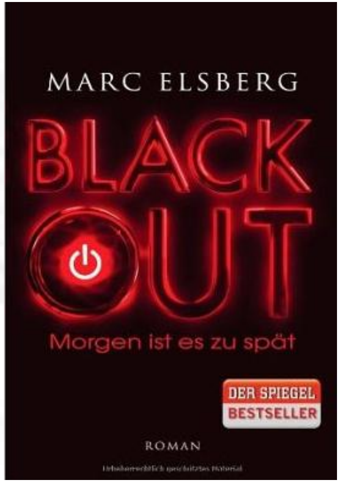
FP7 i-GOing (i-GalilieO indoor navigation): Galilleo like signals by network of pseudolites for indoor navigation

R&D

itrust consulting operates CSIRT Services

Leassons Learned by cofunded R&D project:

- For itrust consulting, R&D is THE enabler of growth.
- Users do not pay the full price for the required security;
  co-funded R&D is mandatory to create the required knowledge to protect against cybersecurity
- Too much competition for R&D funds, an missing focus an result application.
- Missing focus on interdisciplinarity (such as computer and social science to fight against social engineering and usability challenges).
- Missing concerns by operators for Critical Infrastructure Protection and Cybersecurity attacks.



itrust consulting

Thank you for your attention