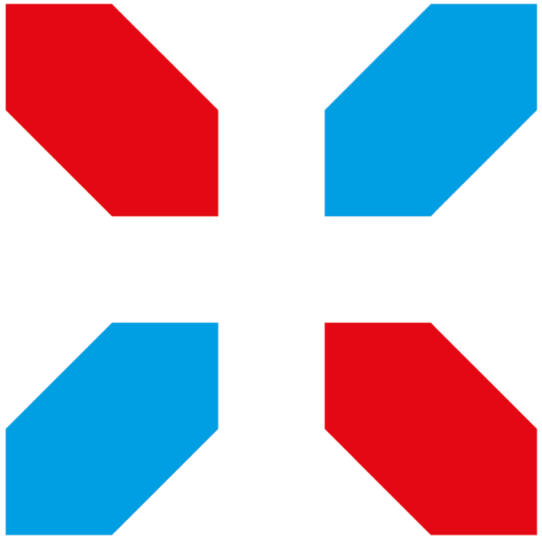
LUXEMBOURG
LET'S MAKE IT HAPPEN

Quels « Cybertools » sont disponibles pour mon entreprise?



Luxembourg
CyberSecurity4Success
October 18th, 2019

c3
Cybersecurity
Competence Center
LUXEMBOURG

A long lasting involvement in cybersecurity matters

LUXEMBOURG
LET'S MAKE IT HAPPEN

- Early leadership of the MinEco in cybersecurity:
  - e-Signature (1999) & e-Commerce (2000) directives
  - 2000: « I love you » virus
  - 2002: OECD Guidelines
    => « Plan Directeur de la Sécurité des Systèmes d'Information », the building blocks of the national cybersecurity strategy
  - 2003: Public service to raise awareness and promote good practice for the entire economy **including SMBs** : acknowledging market gaps and covering them
  - 2006: Nation-wide awareness training in schools
  - CASES : Governance,Risk and Awareness
  - CIRCL : Incident Management & Coordination
- Beyond documentation & awareness, a need for actual tools
  - FOSS and open methodologies support the development of a local cyber security eco-system.

c3 Cybersecurity Competence Center LUXEMBOURG

Agenda

LUXEMBOURG
LET'S MAKE IT HAPPEN

1. Introduction : Why tools ?
2. How to focus on the right tools?
3. Hot issue of the day, for long : email
4. Conclusion
5. Q&A

As we are in a **workshop**, I may also have questions for you !

c3 Cybersecurity Competence Center LUXEMBOURG

LUXEMBOURG
LET'S MAKE IT HAPPEN

The **Cost** of Security !

Security => significant budgets on a recurring basis

- Security => Capabilities
  - People (Governance, Operations – At least)
    - » Hiring
    - » Training
    - » Services
- Security => Recurring spending
  - Endless race with accidental and intentional threats
  - Compliance and contractual obligations

Who can afford a comprehensive security program?

Tools embed know-how and provide capability

c3 Cybersecurity Competence Center LUXEMBOURG

How to focus on the right tools?

LUXEMBOURG
LET'S MAKE IT HAPPEN

- Too many unknowns ?
  - How to make a choice, to allocate budgets ?
    - Internal capabilities : significantly limited
    - Knowledge of exposed assets : significantly limited
    - Understanding of the threats : significantly limited
  - Existing CyberSecurity Market :
    - Still maturing
    - Not affordable for most (hiring or acquiring)
      - » Limited offer (providers & specialists)

Scope ?

Licencing schemes?

Required skills?

- What are cybertools actually?
  - Focused on Internet technologies
  - Bringing Security Capability
  - From online documents to complex systems

c3 Cybersecurity Competence Center LUXEMBOURG

Does it make sense for me?

LUXEMBOURG
LET'S MAKE IT HAPPEN

Digitization

- Progressive & Low visibility
- Suddenly pervasive (Affordable tools & technologies)
- Example of email as core supply chain infrastructure

Common Threats

- Ransomware & DDOS extorsion
- Business Email Compromise & Executives Scams
- Intellectual Property & Strategic Information Theft
- Infrastructure abuse & Third-party targeting
- Mis-management and Mis-configuration

Common Vectors

- Email abuse
  - Phishing
  - Malware distribution
- « Drive by download »

c3 Cybersecurity Competence Center LUXEMBOURG

A practical approach at security planning and tooling

LUXEMBOURG
LET'S MAKE IT HAPPEN

What makes a comprehensive and successful security program ?

- Pragmatism and Persistence are key
- Have a plan, start small, adapt constantly
- Support from execs is critical for credibility
- Involve everyone

Prevention

- **Risk management**
- Access control
- Assets management
- Testing tools
- Backup tools

Detection

- **Monitoring** solutions
- Detection systems (AV's, IDS'…)
- Testing tools

Response

- Incident Response & Forensics tools
- Case management
- Information sharing

BUT Cost !

c3 Cybersecurity Competence Center LUXEMBOURG

How to start ?

- Know yourself : Risk assessment is the key
  - Get advice
  - Ask simple questions
    - Example of a streamlined tool : the CASES Fit4Cybersecurity
    - For more mature organisations : MONARC Risk Mgt Platform
  - Test !
  - Work with your suppliers
  - Don’t be shy about your maturity
- Tools are important but so are skills to operate them
  - Upskills your employees (sustainable)
  - Hire a specialist

Knowing yourself isn't a one time effort !

LUXEMBOURG
LET'S MAKE IT HAPPEN

- Known issue : PenTesting is money and resources intensive
- Proposed solution : C3 Testing platform
  - Initial target = start-up's and SMB's (bigger players are +/- covered)
  - Key issues to be dealt with initially:
    - Email infrastructure
    - IT infrastructure
    - Products and services

C3 Protocols – Level 1

TESTMX

IoT Inspector

  - Objectives : develop **tools and partnerships**
    - Allow and facilitate the emergence of local actors

    => start through a partnership with 2-3 local companies
  - Opportunity for innovation :
    - Beyond identification of gaps, strengthen smaller players in their search for partnerships (investors, institutional customers, business partners) as it allows them to have hard **evidence about their own cyber security competences** without having to face a full certification process.

c3 Cybersecurity Competence Center LUXEMBOURG

Where to go ?

LUXEMBOURG
LET'S MAKE IT HAPPEN

- Security Made In Lëtzebuerg : https://securitymadein.lu/
- C3 Website : https://c-3.lu/
- CASES Website : https://cases.lu/
- CIRCL Website : https://www.circl.lu/
- ROOM#42 simulator : https://room42.lu/
- MISP project : https://www.misp-project.org/
- MONARC solution : https://www.monarc.lu/
- Fit4Cybersecurity : https://startup.cases.lu
- Directory of Open-Source Security Software : https://open-source-security-software.net
- OWASP list of testing tools : https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

c3 Cybersecurity Competence Center LUXEMBOURG

Hot issue of the day, and for long : Email !

LUXEMBOURG
LET'S MAKE IT HAPPEN

- First spam - 3rd of May 1978 - Arpanet - Gary Thuerk
  - Unsolicited Commercial Email
- Now : the main vector for initiating attacks (phishing, scams or malware distribution), i.e.more than #80% of visible criminal activity
- [50 – 60]% of email volume

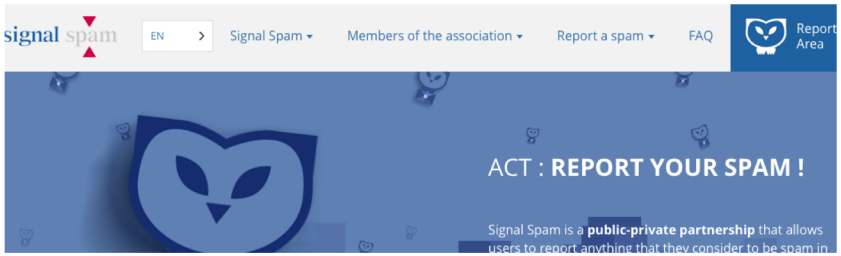
c3 Cybersecurity Competence Center LUXEMBOURG

What has been done against spam?

- Ecosystem-wide
  - Disincentives
- Server level
  - Filters
  - Standards
- Individual user
  - Filters
  - Reporting
- Prevention
  - Awareness

Partnerships !

- Users as active responders
  - Signal-Spam (2004)
    - Spam reporting – Intuitive user experience, once registered
    - Public-Private Partnership
    - No anonymity
  - Phishing-Initiative (2011)
    - Phishing URL reporting
    - Goal : quick take-down and blacklists completion



The next step : SPAMBEE

- Targets : both unsolicited email and phishing
  - Alerting and filtering phishing
  - Investigating abusers
- Privacy by Design : Anonymized Reporting

- Why companies should care?
  - Sharing is caring : identifying campaigns faster
  - Sharing is caring : more effective blacklisting
  - Sharing is caring : better understanding of the threats

- Install SPAMBEE
  https://www.spambee.lu
- Report !

Simple solutions for multilayered security of email

LUXEMBOURG
LET'S MAKE IT HAPPEN

Target	Server testing (Configuration)	Bad email reporting	Phishing Campaign Simulator
• Organisation • People • Infrastructure and Tools	X	X (X)	X X (X)

Server testing	• TESTMX • Internet.nl
Reporting	• SPAMBEE • Phishing-initiative
Phihing campaign simulator	• LUCY • Kingphisher

c3 Cybersecurity Competence Center LUXEMBOURG

Conclusion : How to improve the tools offer ?

LUXEMBOURG
LET'S MAKE IT HAPPEN

- Extend the **platformisation** of basic tools and services
  - Support the development of a broader local offer
  - Rely on sustainable open-source communities around tools
- Offer multi-purposes **toolboxes**
  - Bootstrap Legal & Compliance
  - Communication & Coordination
  - Skills multiplier
- Increase **experiments** and **share**

- Questions
  - Who believes a comprehensive security program is a realistic goal?
  - What are the main constraints to accessing security tools and capabilities?
  - Is the local market providing the right offer?
  - What should be the next priority for developing tools?

c3 Cybersecurity Competence Center LUXEMBOURG

Thank You for your attention !