Contents Presentation

- What is CENTR?
- CENTR GA
- CENTR Jamboree
- CENTR Working Groups
- CENTR Security Working Group
- Security WG Workshop topics
- Security WG Workshop ISO27001
- Secure Contact database and email
- Similarities and differences TF-CSIRT – CENTR SEC
Who am I?

- Bert ten Brinke
- Security Officer SIDN (.nl) since 2009
- In security since 2004
- Expertise: Security Management, ISO27001, Compliance, Risk Management
- I proposed founding of CENTR Security WG
- Chair of CENTR Security WG
- Liaison at National Cyber Security Center
- Secretary of Abuse Information Exchange
- Hobby: Roadbiking
What is CENTR?

CENTR = Council of European National Top Level Domain Registries
CENTR is the main platform for discussion and services to European ccTLD registries

CENTR community
- 52 full members (ccTLDs), 9 associate members and 12 observers
- 80% of country code domain name registrations worldwide
- More than 70 million registrations

Member services
- Dialogue platform via working groups, general assemblies, mailing lists
- Best practice and knowledge sharing
- Policy, news, statistics and industry analysis
- A voice for ccTLDs in the region and the wider internet community
Facts and figures

Milestone in February 2015:
70 million registrations
Benchmarking with peers, online and offline:

- Surveys
- Workshops (six working groups)
- Mailing lists
- Publications
- Statistics
- Joint studies
CENTR General Assembly

- Meeting is organized 2x a year
- Topics are mainly strategic and at board level
- Merely visited by management
- Decision making meetings
CENTR Working Group Charter

- Objective
- Creation, Closure
- Structure
- Chair & Vice-Chair
- Scope
- Budget
- Confidentiality
TF-CSIRT Goals

Forum for where CSIRT community members:

• **exchange experiences and knowledge** in a trusted environment in order to improve cooperation and coordination.

• Maintains a system for registering and accrediting CSIRTs, as well as certifying service standards.

Task force

• Develops and provides services for CSIRT

• Promotes the use of common standards and procedures for handling security incidents

• **Coordinates joint initiatives** where appropriate
CENTR Security WG 1

- Supports and encourages sharing and exchanging of information, ideas and best practices concerning all security-related topics
- Goal
  - improve knowledge on security
  - learn from each other’s experiences
  - inform each other about:
    - new trends
    - possible dangers
    - security incidents
CENTR Security WG 2

- Two physical meetings per year
- Maintains a CENTR Security Working Group mailing list
- Collaboration on specific (joint) projects
- Sharing information about security incidents in a trusted environment
- Code of conduct containing the traffic light protocol
Security WG Workshop topics

- Risk Management
- BCM
- DDOS, Viruses, Botnets, Malware
- 2FA
- Web Application Firewall
- Abuse handling
- Security Intelligence (future)
- Vulnerability Management
- DNS(SEC).
- Employee Security Awareness.
- ISO27001
Examples of presentations

- Awareness game
- Malware free Switzerland
- Dorifell virus
- Risk Management system of CENTR Member
- Hack of .nl, .ie, .be, .rs websites
- Secure Software Development
- CENTR investigation for spam in ccTLD’s
- Amplification attacks ns4.dns.nl
- Implementation of WAF in .be
- www.dafa888.wf DoS attack in .fr
Key static in Motor Management Systeem
Key static in Motor Management Systeem

- No security
- Serial port
- Read and copy
- Trojan in MMS via Wireless, CD of Bluetooth
- BMW, Toyota, Audi, Peugeot, Porsche ...
ISO/IEC 27005:2008 Risk Management
CENTR ISO27001 Workshops

- 2 dedicated workshops, 2 subsequent years
- First workshop in Belgrade:
  - Overview ISO27001 ISMS, basic principles
  - Dedicated chapters as Risk Man, Access Man, BCM
  - Teaching what to do
- Second Workshop in Brussels:
  - For each ISO27001 chapter: Specify topics that are of concern
  - Each topic analysed by subgroups and present it to total group

Result: For each ISO27001 topic enough information to build your own ISO27001 framework
Security contact database and secure email

Contact database
• Purpose: easily find people to communicate about security incidents and other security issues
• Trust is important

Secure email
• Purpose:
  • Facilitate the sharing of (confidential) security information
  • Increase the skill level of participants
  • Minimize the time needed to resolve incidents.
• Trust is important
Similarities TF-CSIRT <-> CENTR SEC WG?

- Security
- Fighting Cybercrime
- Solving Security Incidents
- Making the internet better
- Sharing information, knowledge, best practices
- Learning from each other
- Security Management process
Differences Topics TF-CSIRT <-> CENTR SEC?

- End Customer
- TF-CSIRT might be more technical
- CENTR has also TECH community
- CENTR SEC is much smaller