CERT.PT
Serviço de Resposta a Incidentes de Segurança Informática

A rede nacional de CSIRTs

Workshop "Cibersegurança: aspectos económicos"

Lino Santos

FCCN
Fundação para a Computação Científica Nacional

CERT.PT
Serviço de Resposta a Incidentes de Segurança Informática

Agenda

1. CERT.PT
2. Rede Nacional de CSIRTs
3. Auto-avaliação
4. Conlcusões

FCCN
Fundação para a Computação Científica Nacional

CERT.PT
Serviço de Resposta a Incidentes de Segurança Informática

CERT.PT

O CERT.PT tem como missão contribuir para o esforço de cibersegurança nacional nomeadamente no tratamento e coordenação da resposta a incidentes, na produção de alertas e recomendações de segurança e na promoção de uma cultura de segurança em Portugal.

CERT.PT

Serviço de Resposta a Incidentes de Segurança Informática

Malta
Moldova
Montenegro
Slovenia
Netherlands (Tl
Norway
Poland
Portugal
Romania
Russian Federa

Financial Sector
Governmental / Milit
National, Research
Service Provider Cu
Non-Commercial Or
ISP Customer Base
ICT Vendor Custom
Commercial Organi
Industrial Sector
Major Service Provi

Use the key combination CTRL+Select for multiple

Generate report

N/G CERTs report

Portugal :

Research and Education
CSIRT.FEUP
Establishment date: 02/03/2006
Contact: http://csirt.fe.up.pt
TI Status: accredited
FIRST Membership: not member

ISP Customer Base
csirtPT
Establishment date: 04/01/2010
Contact: http://csirt.telecom.pt
TI Status: accredited
FIRST Membership: not member

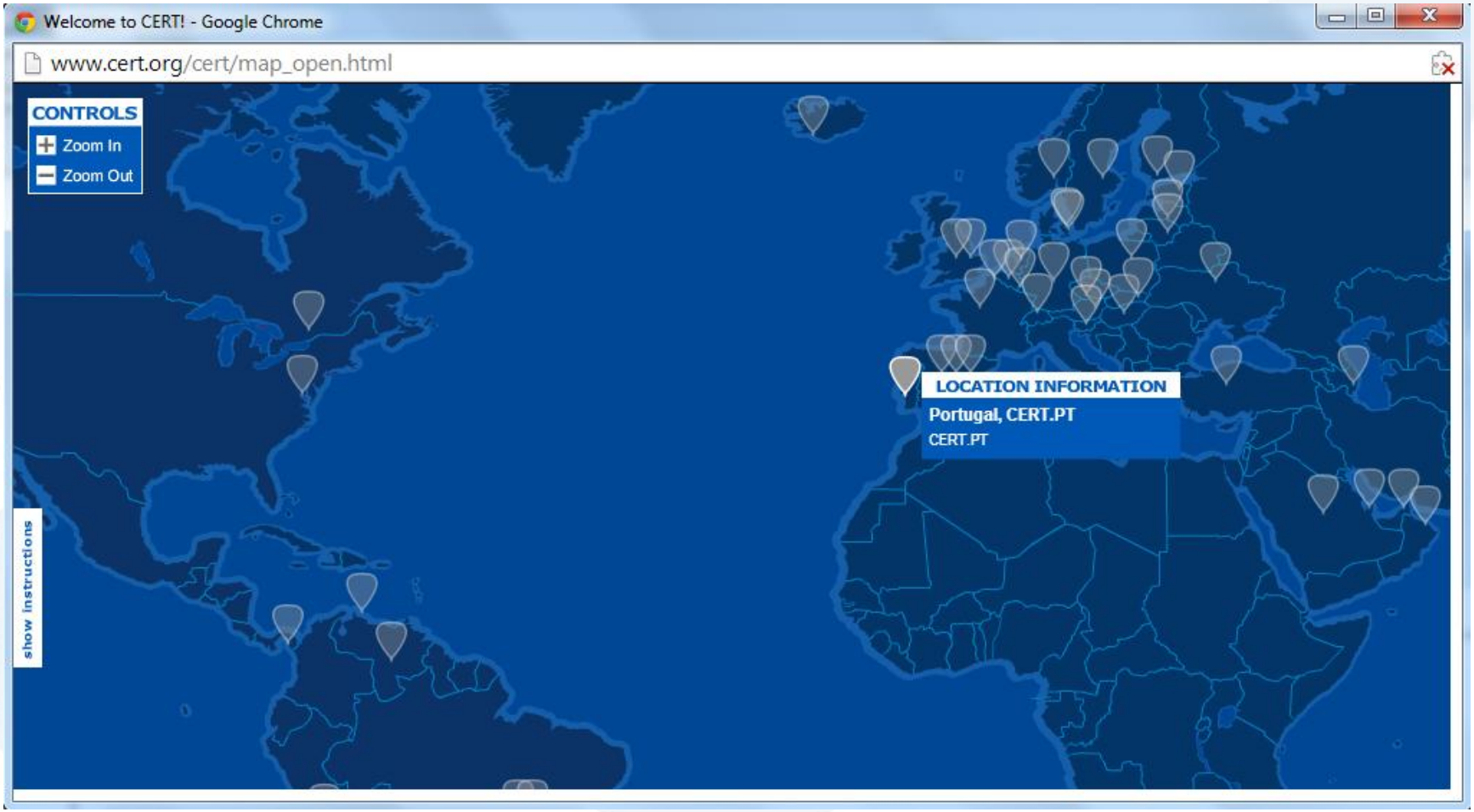
Vendor Customer Base
DGS-IRT
Establishment date: 01/01/2005
Contact: https://www.dognaedis.com/
TI Status: accredited
FIRST Membership: not member

De Facto National
CERT.PT
Establishment date: 14/10/2002
Contact: http://www.cert.pt
TI Status: accredited
FIRST Membership: member

Back to CERT Inventory

CERT.PT
Serviço de Resposta a Incidentes de Segurança Informática

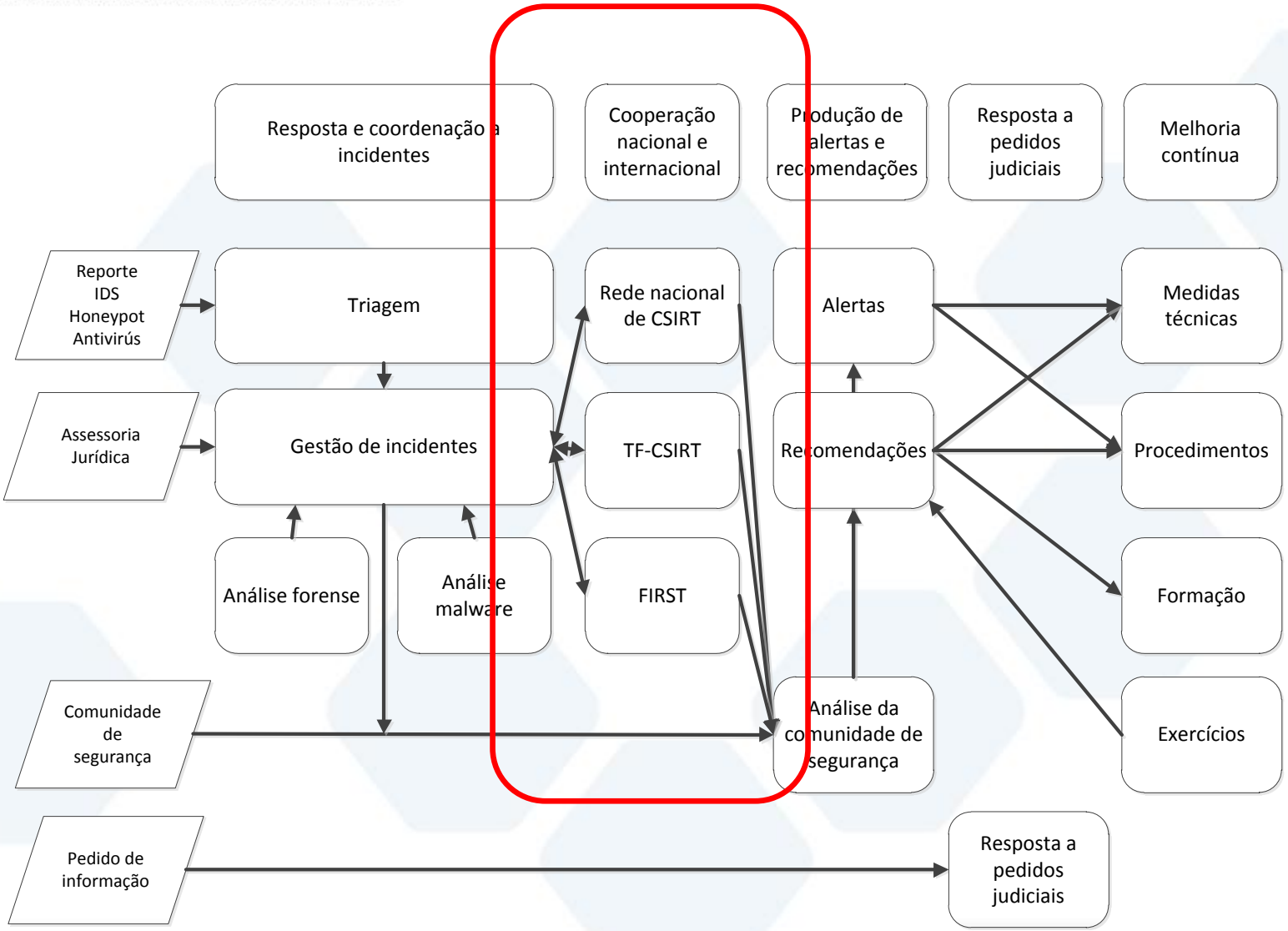
CERT.PT



UMIC
Agência para a Sociedade do Conhecimento

FCCN
Fundação para a Computação Científica Nacional

Processos CERT.PT



A tentativa falhada

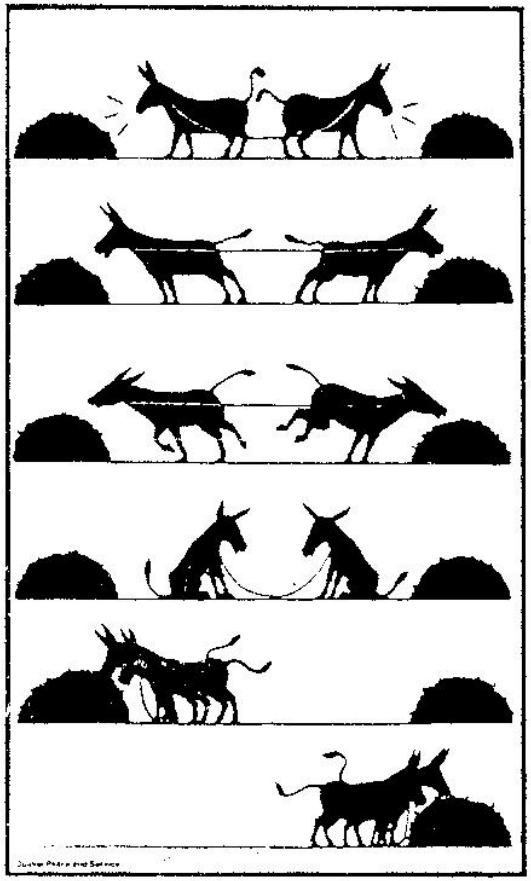
- 2006 – fórum sobre segurança com o ISPs
  - Modelo ad-hoc sem objectivo definido
  - Nenhum ISP sabia o que era um CERT
  - O tema do momento era o anti-SPAM
- 2007 – aposta na formação e evangelização
  - Oferta de dois cursos sobre resposta a incidentes
  - Divulgação do conceito CERT
  - O “caso da Estónia” saiu da esfera dos “geeks”

Os primeiros passos

- Jan 2008 – Protocolo de cooperação em matéria de segurança com a Sonae.com
  - Auxílio mútuo na resposta a incidentes de segurança
  - Partilha de informação de segurança
  - Criação da Rede Nacional de CSIRTs

- No final de 2009 a Rede Nacional de CSIRT contava com 7 membros

Rede Nacional de CSIRT



- Criar um ambiente de cooperação e assistência mútua no tratamento de incidentes
- Criar indicadores e informação estatística
- Criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão

Membros

- Academia
  - CSIRT.FEUP, INESC
- ISP
  - Sonaecom, Cabovisão Clara.net, Portugal Telecom, ONI, REFER, Vodafone
- Forças armadas
- Banca
  - BCP, CEMAH, CGD
- Operadores IC
  - EDP
- Administração pública
  - IGFEJ, DGIE

CERT.PT
Serviço de Resposta a Incidentes de Segurança Informática

Criar um ambiente de cooperação e assistência mútua no tratamento de incidentes

- Como não fazer...
  - Estrutura hierarquica para reportar incidentes
  - Eg. Euro-CERT (1998-1999)
- Grupos ad-hoc
  - Conficker, Kaminsky, ...
- Comunidades de interesse
  - TF-CSIRT, ICANN, FIRST, FI-ISAC
  - Maior enfoque em objectivos concretos

Criar um ambiente de cooperação e assistência mútua no tratamento de incidentes

- Como não fazer...
  - Definir objectivos rígidos e ambiciosos
  - Interesses distintos
- Começar pequeno e depois crescer
- Definir conceitos e processos
- Ter cuidado com atitudes passivas

Criar um ambiente de cooperação e assistência mútua no tratamento de incidentes

- Instrumentos criados
  - Quatro reuniões anuais
  - Seminário anual
  - Workshops temáticos / Formação / Projectos
  - Código de conduta dos membros
  - Taxonomia comum
  - Boas práticas na resposta a incidentes
  - Falsidade informática, Interferência em sistema e Interferência em dados

Criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão

- Necessários processos montados e testados
  - O treino é feito no tratamento de incidentes comuns
- Nessessária uma boa rede de contactos
- Necessários instrumentos de comunicação segura e colaboração
- Necessário um processo de escalagem

Criar os instrumentos necessários à prevenção e resposta rápida num cenário de incidente de grande dimensão

- Instrumentos criados
  - Base de dados de contactos
  - Formato de troca de incidentes baseado em standard IODEF para automatização de processos
  - Mecanismo seguro para troca de informação baseado em PGP
  - Adaptação de ferramentas

Criar indicadores e informação estatística

- Recolha mensal de indicadores (números) de incidentes tratados por tipo
- Os valores mensais de cada um dos membros são anonimizados para produção de indicadores da Rede

Proposta de plano de actividades para 2013-2014

- Criação de ferramentas para promover a partilha de informação e o auxílio mútuo
  - Adopção do protocolo TLP
  - Criação de um whois privativo
  - Criação de uma knowledge base
  - Ferramenta de IM segura
- Definição de SLA entre CSIRTs
- Criação de um modelo de governance

CERT.PT
Serviço de Resposta a Incidentes de Segurança Informática

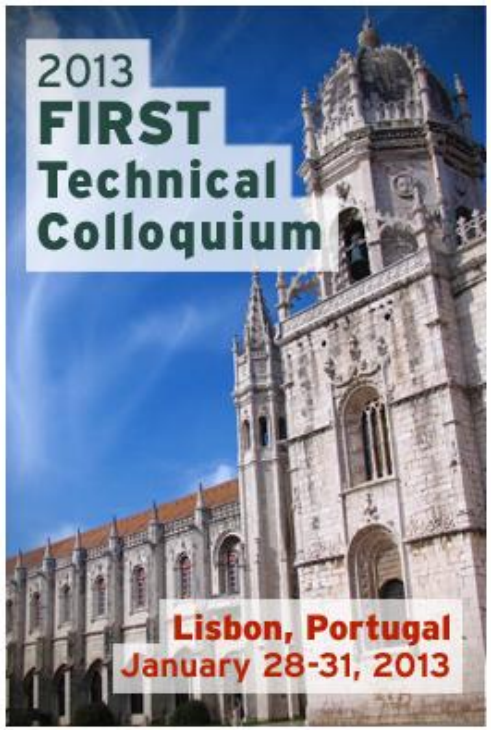
Lisbon 2013 FIRST/TF-CSIRT Technical Colloquium

Lisbon (PT), 28 – 31 January, 2013

FIRST Technical Colloquia & Symposia provide a discussion forum for FIRST member teams and invited guests to share information about vulnerabilities, incidents, tools and all other issues that affect the operation of incident response and security teams.

For you that are new in FIRST or never have attended a TC, the colloquium typically provides one whole day of plenary sessions for informal discussions and presentations on topics of FIRST membership interest, or that are more sensitive in nature and related to the day-to-day work of participants.

The FIRST colloquia are typically hosted by members and since 2005 are being organized in a regional basis - the current regions being Latin-America, North-America, Europe and Asia-Pacific. For each region the goal is to organize one TC per year - either standing on its own, or jointly with regional CSIRT initiatives.



Location

The event will be held at the **Laboratório Nacional de Engenharia Civil (LNEC)**, located at:

Av. do Brasil, 101
1700-066, Lisbon
Portugal

Click on the map to see it enlarged on Google Maps.

UMIC Agência para a Sociedade do Conhecimento
FCCN Fundação para a Computação Científica Nacional

Auto-avaliação

E o que acham os actuais participantes na Rede Nacional de CSIRTs?

Aspectos positivos/sucessos

"Conhecer as pessoas facilita a confiança"

"Elevado grau de confiabilidade"

"Partilha de experiências vividas e processos de mitigação"

"Canais directos entre os vários participantes ao nível operacional"

Aspectos positivos/sucessos

“aprendemos muito”

“partilha prévia de informação em casos de ameaças”

Aspectos negativos/dificuldades

Dificuldades internas: “Sponsorship da administração insuficiente”, “articulação com o negócio”, “(in)cultura de segurança”

“Modelo funcional da Rede constitui barreira para a sua afirmação”

“falta partilha de informação sobre ataques sofridos”

“diferentes níveis de maturidade e de preparação”

Aspectos negativos/dificuldades

“heterogeneidade das organizações”

“falta de governação que possa tutelar as posições dos diversos atores”

“precisamos de mais activos para desenvolver o nosso trabalho na rede”

Conlcusões

- A cooperação e a partilha de informação não se fazem por decreto
- A confiança nas pessoas é central
- Demora muito tempo a construir essa confiança
- Existem vantagens e desvantagens num modelo de cooperação semi-formal de adesão voluntária
- A partilha de informação é uma questão cultural... A cultura Internet

CERT.PT
Serviço de Resposta a Incidentes de Segurança Informática

obrigado!

UMIC
Agência para a Sociedade do Conhecimento

FCCN
Fundação para a Computação Científica Nacional