Poste Italiane CERT: Strategy, Mission, and Services

40° TF-CSIRT Meeting
London, 27h September 2013
<table>
<thead>
<tr>
<th>Agenda</th>
<th></th>
</tr>
</thead>
</table>
| **SCENARIO** | • Poste Italiane and Digital Services  
|           | • Cyber Security Scenario |
| **STRATEGY** | • Poste Italiane Leadership in Cyber Security  
|            | • Integrated Approach to Cyber Security: CERT |
| **SERVICES** | • CERT Poste Italiane Activities  
|            | • CERT Services and Cooperation Networks |
Poste Italiane is one of the main Italian organization with 144,000 employees, 13 Mln of online customers and a widespread presence in Italy with 12,000 post offices. It provides financial, logistics, postal, insurance, digital communication, mobile and TLC services.

With 144,000 employees, Poste Italiane is the largest Italian company and State owned enterprise.

Poste Italiane’s customers are citizens, Public administrations and private enterprises.

Poste Italiane provides traditional and new services through internet and mobile channels.

Poste provides e-finance, e-government, e-commerce, e-post digital communication services.

POSTE ITALIANE NEEDS

- **Protecting customers** is a top priority in Poste Italiane business strategy.
- Providing **secure and continuous services** is essential to guarantee customer satisfaction.
- More and more sophisticated cyber attacks working on a global scale call for a deeper **cooperation at international level**.
The evolution of the Cyber Security scenario calls to define a strategic approach

**World increasingly interconnected**
- The technology pushes toward never ending interconnections
  - People, machines, things
  - Big data
- The Society has never been so open and connected
  - PA and Institutions
  - Companies & People

**New threats scenarios**
- New criminal actors (governments, enterprises, cyber-criminals, ...)
- Globalization of attacks vs. local defense
- Industrialized attack processes (ex. hackers “for rent”)
- Advanced threats attacks (mobile devices, cloud, WiFi, big data, IoT)

**Increase target to be protected**
- Public sector
- Private sector
- Citizens
- Critical civil and military infrastructures

**Legislation evolution**

**EU CYBER SECURITY STRATEGY**
The proposed NIS directive (February 7, 2013) would require all Member States to:

- Achieving cyber resilience
- Drastically reduce cybercrime
- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

**ITALIAN GOVERNMENT**
A decree of the President of the Council of Ministers (January 24, 2013) sets forth the new government architecture that is entrusted with the task of facing potential cyber security threats in Italy.

- Italy has a new cyber security governance, pursuant a more precise accountability among governmental bodies and also opening to non public actors
- Italy has to develop a national cyber security plan: the Prime Minister is in charge of adopting the plan.

Operators who manage critical infrastructure at national and European levels:
- send communication of each and every security or integrity breach
- use the best practices as well as cybersecurity measures;
- supply information to security information bodies
- grant access to the database for the purposes of cybersecurity
- assist in managing the cybernetic crisis.
The evolution of the Cyber Security scenario calls to define a strategic approach

**New strategic challenges**

The **Cyber Security** must be a **strategic priority** at Country level, under a European / international common framework:

- **Governance** and well established role system
- Real time **monitoring** and **sharing** critical incident response through **information** to key stakeholders
- Increase **people awareness** (culture, competences, behaviors)
- Promote advanced Cyber Security capabilities through stimulating **innovation industrial clusters** on prevention, even through PPP

**POSTE ITALIANE CYBER SECURITY STRATEGY**

Has focused on **cyber security as a strategic leverage** to provide secure services and protect customers, on-line services and transaction, acquiring an acknowledged leadership at national level

- **TO PROTECT** company’s network and infrastructures, while **preserving customers privacy, on line services and service usability**
- **TO STRENGTHEN** collaboration between public and private stakeholders to contrast cyber crime
- **TO INCREASE** cyber security capabilities through **research, education and awareness**
- **TO INTEGRATE** and coordinate **prevention, analysis and response** capabilities through a unique interface

**POSTE ITALIANE NEW OPPORTUNITIES**

As one of the **most advanced player in the cyber security** field, Poste is in a great position to deliver cyber security services to the market

- **Prevention and protection** services, specifically addressed to **SMEs**
- **National / local cyber security services** might be **delegated** from PA bodies to market operators
- **Educational formats**, deliverable through physical or virtual channels
- Existing or **new offering** (ex. **Cloud**) integrated with **high level security standards**
To integrate and coordinate prevention, analysis and response capabilities through a unique interface

To increase cyber security capabilities through research, education and awareness

To strengthen collaboration between public and private stakeholders to contrast cyber crime

To protect company’s network and infrastructures, while preserving customers privacy and service usability

To protect company’s network and infrastructures, while preserving customers privacy and service usability

Monitoring capability to intercept ongoing attacks and react to IT incidents

• Continuous monitoring
• Anti-Fraud
• Anti-phishing
• Anomalous behavior

Enhance security through cooperation and Information Sharing

PPP – Public-Private Partnership between law enforcement, academia, legal, and private sector

• Contribute to international policies
• Education and awareness
• Cooperation on cyber security with ISO, ICANN, NATO
• MSc in Cyber Security

Aggregate competencies, integrate information flows, share intelligence on ongoing attacks

Standardization of security services to support internal constituency and third parties

Goals

Achievements

Security Room, Fraud Management & Service Control Room

European Electronic Crime Task Force

Cyber Security Center

Computer Emergency Response Team

2006

2009

2010

2013
The experience acquired has led to a new concept of integrated defense: CERT

**Mission**

“to provide a unique point of coordination of all the activities related to prevention and handling of cyber threats impacting the information assets of Poste Italiane, by an integrated management of all the relevant flows coming from each of the already active operation centers, and to represent, at the same time, a unique interface towards the outer world with reference to all the operative information exchange activities”

**Constituency**

“refers to the Poste Italiane Group, the relevant online services and its Customers, including the holding and the affiliates: Poste Italiane SpA, Postecom, PosteMobile, Postel, PosteShop, PosteTutela. This initial constituency is planned to grow, in order to include all of the other entities belonging to the Group.”

---

**The 1st Computer Emergency Response Team (CERT) was created by Carnegie Mellon in 1988 at DARPA’s direction in response to the Morris Worm**

**European Agency on Network and Information Security, whose mission is to support the creation of CERTs in Europe and to foster networking**

**Trusted Introducer is the European CERT network, a service infrastructure whose mission is to provide support for all security and incident response teams.**

**FIRST is the recognized global leader in incident response teams worldwide coordination and is the reference global network for CERT cooperation**
CERT Poste Italiane activities: Monitoring, Analysis and Simulation

**Security Monitoring**

Real-time continuous monitoring of security status of systems and vulnerabilities in the wild, with the aim of detecting new potential attacks or security criticalities and give the start to effective response activities.

**Analysis & Prevention**

Analysis and correlation of collected evidences and alerts coming from the monitoring activities, with the aim of preventing security incidents that may occur on IT systems and services, assessing their potential impact on business.

**Modeling & Simulation**

Definition of mathematical models and algorithms to evaluate potential IT impacts of cyber security threats, by simulating their spread over the company’s network and delivering worst-case scenario analyses.
CERT Poste Italiane Service Offering

INFORMATION
- EARLY WARNING
- INFORMATION SHARING

OPERATIONS
- INCIDENT HANDLING
- THREAT AND VULNERABILITY MNGT

GOVERNANCE
- INFORMATION SECURITY RISK MNGT
- PRIVACY COMPLIANCE

CYBER CRIME
- ANTI MALWARE-PHISHING-SPAM
- SECURE DIGITAL IDENTITIES

CYBER LAB
- CYBER SECURITY TECHNOLOGY LAB
- TECH. COMPLIANCE & SEC. CERTIFICATION

COMMUNICATION
- TRAINING AND AWARENESS
- ABUSE DESK

Alerting services on cyber security issues and information exchange within all the relevant international communities of peers

Operational security activities such as incident handling and analysis of actual protection of IT infrastructures and digital services

Business Impact Analyses, realization of Risk Assessment and verification of process compliance to Data Protection legislation

Monitoring and prevention of threats and ongoing attacks, to also support the repression of crimes against customers’ digital identities

Laboratory activities aimed at scouting innovative security technologies and assess technical compliance to international standards

Awareness and training on information security topics towards both customers and CERT’s constituency
The Early Warning service aims at providing alerts to the PI CERT constituency

**Main Goal**

Early Warning aims at **identifying**, **analyzing** and **promptly reporting** emerging vulnerabilities and threats that may impact CERT constituency, also providing countermeasures for their mitigation.

---

**Information Gathering**

- SecurityFocus.com
- NIST
- cve.mitre.org

**Information collection:** Vulnerability information are collected from various sources, such as:
  - Vendor vulnerability product information
  - Websites
  - Public and closed mailing lists

---

**Analysis**

**Analysis of information collected:**
- Trustworthy of the source is evaluated and further and deeper analysis are performed
- Information are filtered and classified basing on the criticality of the vulnerability reported

---

**Vulnerability Alert**

**Distribution of information:**
- Bulletins templates are filled with the information processed
- Vulnerability alerts are distributed to the constituents

---

Early Warning alerts will be available on the PI CERT web portal.
The Information Sharing service is designed to collect and exchange information on strategies, best practices and cyber crime trends.

It is structured in three main services:

1. **Threat Intelligence**
   - Threat analysis, including implications and actionable advices, about an existing or emerging techniques by means of direct involvement of internal and external security research centers.
   - Deliverables:
     - Threat Analysis Report
     - Technology Watch Report
     - Flash Report

2. **Incident Investigation**
   - Investigation of security incidents with an impact on networks under monitoring, through correlation of information from public and private sources, aimed at threat identification, quick response and mitigation.
   - Deliverables:
     - Incident Report Sharing
     - Flash Report

3. **Communication Center**
   - Collection, analysis and dissemination of IT security related topics within all constituency and the relevant world communities of peers.
   - Deliverables:
     - Early Warning Bulletins
     - Actionable Intelligence IS
     - Knowledge Base
     - EECTF Newsletter
     - Trusted Networking Hub
PI-CERT strategies in the short-medium term

• OPERATIONAL CONSOLIDATION
  As a newborn organization supporting a large Group we have been investing to consolidate our internal processes and to formalize interactions within our constituency, in order to also properly design the relevant services and the underlying infrastructure

• GLOBAL COOPERATION
  We have joined several international communities to foster information sharing of operational data and co-operate on incidents involving Italian critical information infrastructures
  We are ready and willing to cooperate with TF-CSIRT community, sharing information, providing capabilities and developing joint analyses

• INTERNATIONAL ACKNOWLEDGEMENT
  We have a roadmap to become FIRST affiliate and accredited TI Members by the end of 2013

• CONTINUOUS IMPROVEMENT OF COMPETENCIES AND SKILLS
  TERENA training sessions and other international events
THANKS A LOT FOR YOUR ATTENTION

ANY FURTHER INQUIRY CAN BE SUBMITTED TO

cert@posteitaliane.it