Cyber-eS 2014

Executive summary

An initiative of

CNPIC

CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

With the collaboration of

ISMS Forum Spain

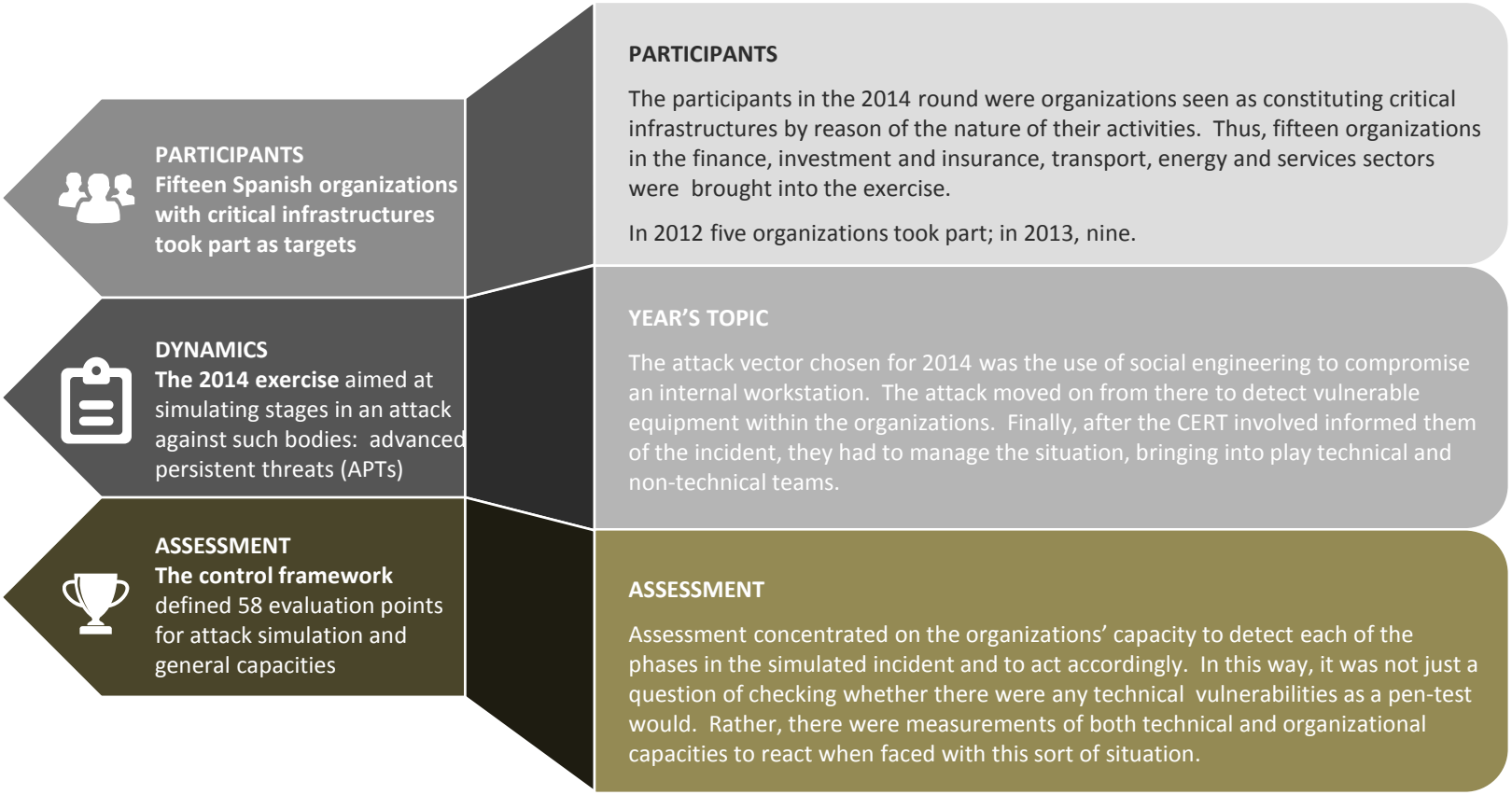
- Method
- Analysis & General Recommendations

Method

certsi_
CERT DE SEGURIDAD E INDUSTRIA

General Description of CYBER-EX 2014

The CYBER-EX are the national cyber exercises for the strategic sectors and critical infrastructures. This initiative is promoted by the Spanish National Cybersecurity Institute, that depends of the Ministry of Industry, and the National Centre for the Critical Infrastructure Protection, that depends of the Ministry of Interior. This initiative is included in the National Cybersecurity Strategy and the Spanish Digital Agenda.

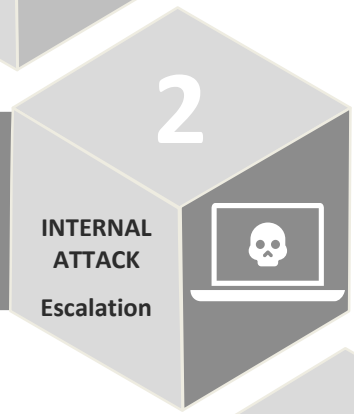


certsi_
CERT DE SEGURIDAD E INDUSTRIA

Attacks and Dynamics: Simulating an APT

INITIAL VECTOR: SOCIAL ENGINEERING
The first stage of the attacks involved sending fake e-mails to get information about the organizations (phishing). The starting point for attackers was seeking out e-mail addresses in the organizations' web-pages, after which these were used to send the spurious messages.

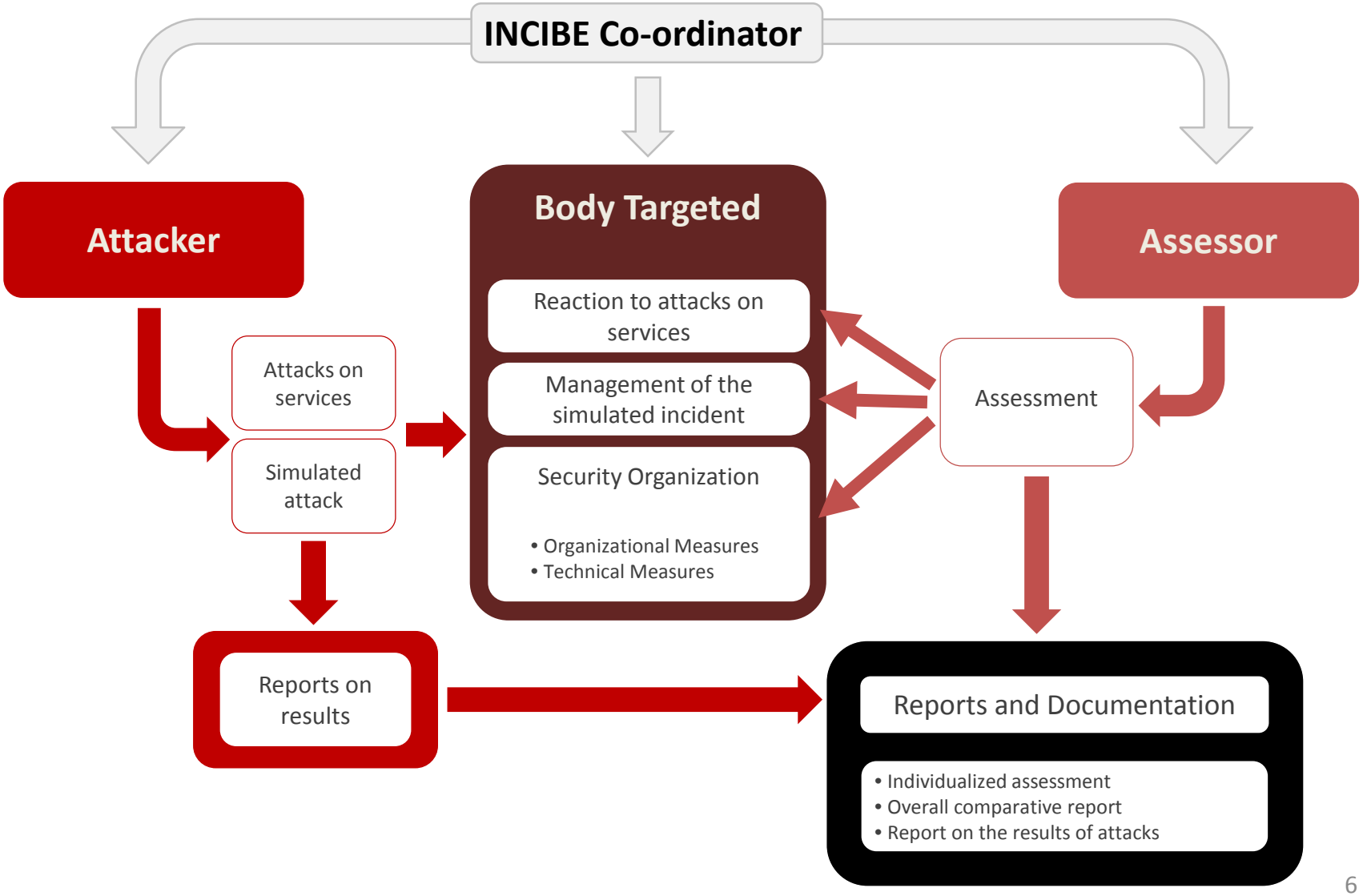
PROGRESS OF ATTACKS THROUGH THE INTRANET
To simulate the effect of successfully compromising a machine connected to the organizational intranet, a controlled attack was made from a connection to the local area network of each body targeted, in an attempt to detect vulnerable equipment and possible objectives for more sophisticated or directed incursions.



RESPONSE TO SECURITY INCIDENTS
Finally, a **simulated table-top exercise** was used to measure the capacities for responding to and managing an incident notified by the Security and Industry CERT. Teams had to cover both technical responses to the crisis and communication about it with third parties (CERT, the press, and so forth).

certsi_
CERT DE SEGURIDAD E INDUSTRIA

Roles



Assessment System

- A set of 58 checks was defined, divided into several groups. These were used to assess each of the organizations participating.
- Assessments were based on attackers' reports.
- The scores awarded reflected the level of implementation of the framework of checks n the target organization.
- Assessments of these checks are to be found in detailed form in the section on "individual assessment" , along with any relevant comments.
- Scores running from 0 a 10 were awarded as a function of the degree of implementation of the check.

- There were two types of assessments for checks.
  - Binary assessments: 0 it the check was not in place, 10 if it was.
  - Scaled assessments: 0 to 10, with values increasing as the check became more effective.

- *Specific Points about the Cyber-Exercise:*

  - Fifteen organizations participated as targets.
  - Technical attacks for each of the services at risk were carried out by the same team of professionals for all the participants.
  - The assessment team was the same for all the participants.

Analysis & General Recommendations

- Attacks, Phase 1: Vectors for Gaining Entry to the Organization – Social Engineering
  - Anti-Phishing Filters: It is recognized that at the present time many employees fall victim to phishing despite awareness-raising campaigns run by their businesses. The most effective way to avoid this problem is to put in place an anti-phishing system so as to filter out malicious e-mails automatically. This should be combined with the implementation of mechanisms like Sender Policy Framework (SPF), along with training to allow workers to distinguish genuine from fake contacts.
  - Raising Awareness: There is place for improvement in the area of awareness-raising relating to social engineering. Stress should be laid on the fact that merely by going to malicious web-sites a machine with vulnerabilities may be compromised.

- Attacks, Phase 2: Progress of an Attack – Tests for Internal Intruders
  - Insiders: A scan for vulnerabilities carried out within an internal network is a serious security incident. It is a very different scenario from a scan undertaken from an external network like the Internet, since the attacker must be either a worker or an associate of the organization, or somebody who has succeeded in penetrating its perimeter defences. The recommendation would be to increase detection and containment measures against this sort of incident as soon they are detected, as also to add access control mechanisms wherever these are not already in place.

- Attacks, Phase 3: Investigation of Incidents - Table Top
  - Categorization: On some occasions no proper labelling is created in the system so as to document incidents correctly, which suggests that here too there is room for improvement in the management of security incidents.
  - Forensic Image: It is highly advisable to take screenshots of any infected workstation so as to conserve evidence.
  - IOC: It is recommended that IOC should be generated and communicated to INCIBE and other Computer Emergency Response Teams (CERTs) when security incidents which are like those simulated occur.
  - Issue of Reports: It is recommended that a report should be drawn up with the conclusions reached and actions undertaken as the security incident was managed so as to record the lessons learnt from the situation undergone.

- Organizational Measures:
  - High-Level Organizational Measures: In general, the degree of maturity of the organizations in the field of organization of security was high. Nevertheless, it would be advisable to increase efforts to measure security levels (KPI).
  - Defining and revising indicators at intervals is an essential task in achieving proper security management.

- Technical Measures:
  - Reviewing Metadata: It is advisable for a metadata review process to be included before the publication of any documents.
  - Life-Cycle of Vulnerabilities: Tools should be available to manage the life-cycle of vulnerabilities
  - Encryption of Internal Communications: The most recent models for security stress the fact that it should be accepted that breaches of security will occur. To increase the resilience of a company, it is wise to implement encryption in internal networks, at least for the most sensitive or critical protocols and services, such as intranet web services or communications with ERPs and business databases.
  - Information Leaks: To reduce the likelihood of information leaks, DLP or IRM solutions might be adopted. Furthermore, it is highly advisable to keep tabs on extractable media such as USB drives so as to prevent information leaks, as well as eliminating a malware entry vector.

Cyber-eS 2014

An initiative of

CNPIC
CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

With the collaboration of

ISMS Forum Spain