Welcome to LR

Information Security and Cyber security on Ships
Genova 28-06-2017
Ilaria Savini

Lloyd's Register
LRQA

Improving performance,
reducing risk

AWARENESS

Why cyber security

There are two levers for moving men: interest and fear

Napoleon Bonaparte

The importance of security

The cyber defense is a top priority for NATO: the General Secretary l of the Atlantic Alliance points out in Brussels recently Last year - said Stoltenberg - NATO has had an average of 500 per month cyber incidents that required a response from our experts."

CLUSIT (Italian Association on Cyber Security) 2016 Report on Information Security in Italy, in Europe and around the world asserts that 2016 was the worst year ever in terms of the evolution of cyber threats and their impact.

Cybercrime cost : 2013 $ 100 billion (Wall Street Journal)
2014 $ 300 billion (Mc Afee)
2015 $ 400 billion (Lloyd's)
2016 $ 500 billion (Allianz)
2017-2019: estimate $ 2 trillion (Juniper Research)

I wanna cry……

150 COUNTRIES, go phut thousands computers with not Windows updated software

Ransomware:

Ransomware (also called rogueware or scareware) limits access to a user's computer system and requires payment of a ransom to remove the block. If you are affected and infected by a ransomware, you will no longer be able to access your computer

What is important?

All software on your computer (or mobile disposable) needs to be up-to-date, including operating system, browser, and various plug-ins. And backup

Prevention: Constant update of antivirus and firewall.

I wanna cry……

WHAT HAPPEN:

1) Victims receive malware on the net (there is currently no virus vector evidence of infection);

2) Malware installs into the 'victim' machine by exploiting the known bug

3) then installs as a service and performs two parallel activities using several executables;

4) The first activity is to encrypt certain types of files

5) The second activity is to propagate the malware on any LAN present, exploiting the protocol vulnerability. This second component also scans over the network to search for new targets to infect;

And now PETRWAP

New global attack started from Russia and Ucraina but arrived also in France, Denmark and UK and in the world.

The virus has attaked: Kiev Airpot, Kiev underground, Kiev central train station, Kiev central Bank, Ucraina national power plant and distribution energy company; Chernobyl nuclear power plant (the attch was directed to the automatic radiation monitoring system now changed in manual operating), the most important Russian oil company Rosneft, the most important advertising company in the world WPP, the danish shipping company Maersk (paralyze several terminal in the world, the last is the Jawaharlal Nehru Port (JNPT), the bigger in India for containers traffic).

…and many others.

Each people have received a Messages to pay ransoms in Btcoin ($300.00)

How does it work?

The troll entered into the system as a normal email.

The troll (ransomware) attacks the central operating system to find files, making them unusable definitively .

The troll steals personal data and blocks profiles.

In fact virus offs the computers.

And now PETRWAP

TRY TO THINK TO THE DAMAGE (ECONOMIC, FINANCIAL, OPERATIVE, IT, OT, HUMAN RESOURCES, CLIENT CARE, IMAGE)

TRY TO THINK TO THE COSTS

WHY DO NOT INVEST IN CYBER SECURITY?

What we can do

A ship in harbor is safe, but that's not why the ships were built.

(John Augustus Shedd)

Certification or Assessment

- Different goals and targets, different implementing rules
- **Certification** has a tactical purpose, a tactical aim (a contract, a tender, a market ...)
- An **assessmen**t can have different purposes as needed:
- Understanding the state
- Analyze weaknesses
- Identify weaknesses
- Having an independent opinion regarding something
- Gather information to take decisions

Information security management

Risk assessment

- Identification of risks;
- Analysis and evaluation;
- Selection of control objectives and control activities for risk management;
- Taking the residual risk from the management;
- Definition of the Statement of Applicability. It may, for instance, take the form of a matrix identifying various types of information risks on one axis, and risk treatment options on the other, showing how the risks are to be treated in the body, and perhaps who is accountable for them

Different kinds of assessment

Main assessments based on:

- International and National standards
- Technical Standards ISO (27k, 20k, 22301), ETSI, EN, IEC….
- Guidelines (ISA/IEC 62443 and other)
- Framework (NIST- National Institute of Standard and Technology: Cyber security Framework)
- VA/PT (OSSTMM, OWASP, …)
- International and National rules (particularly from UE)
- Data protection, Privacy, …
- Referring to contracts or companies'standard

Adding Value to Clients
From compliance to performance

Adding Value to Clients
From compliance to performance

VA:
Exhaustive search to identify as many vulnerabilities as possible within an environment. The assessment measures and rates the level of risk that potential scenarios may present to a system.

PT:
A PT simulates an actual cyber attack by employing the same techniques and methods used by hackers. Pentest can be very invasive because the objective is often to gain unauthorized access to systems by exploiting vulnerabilities. Special precautions must be taken when testing systems.

Adding Value to Clients
From compliance to performance

- **Customer Choice:**
- **White box** :some information are shared and everything is agreed. E.g: You can see the behavior of infidel employees. They give you user passwords and you can see if you can scale accesses. If you know a password ... what can happen ?
- **Grey box :** some information are shared I can get information through social engineering)
- ,**Black box :** I act as if it were a real attack, I do not get information and I do not share information. You acquire the information from the outside, I work on the previously identified vulnerabilities

The context: ICT (Information & Communciation Technology) & OT (Operational Technology)

Relations in terms of cyber security, including all organizational contexts, whether ICT (Information & Communication Technology), or OT (Operational Technology), or operational or compliance are increasingly close.

Referring to the assessments on cyber security, thinking to deal with each area with **the same approach and the same models it's a mistake**, even if the underlying operating strategies are common .

An example? Apply the use of firewalls, designed for Web Application and traditional IT facilities, in industry (OT), it would not be fully effective as protocols, rules, and ports are different and typical of the devices connected to the plant network and control systems /remote control..

It means that the different types of assessment must be applied in distinct areas, adopting methodologies dedicated, specific instruments, adequate professionalism and standard processes.

OT Assessment

- Difference between security in the world of cyber physical systems and traditional cyber security:

- The OSSTMM methodologies are designed for digital systems
- **The goal of the hacker is NOT the extraction of the data but to see whether it is possible to take control of the digital system machines**
- **PT in SCADA systems** (supervisory control and data acquisition) or or DCS (Distributed Control System) **tends to investigate whether via electronic access you can create a physical problem.**
- What hackers are interested in? Eg. Embedded on engine: the hacker does not affect access to software or the embedded data, but interested in what I can do on the enginee, system, automation system etc.
- Hackers want to create highly visible incidents that embarrass or harm companies

OT ASSESSMENTS

- SCADA systems are the heart of the company and when it does a VA PT is a significant problem on interruption or on the possibility of creating a disservice
- Despite the issues involved, it is possible to conduct meaningful penetration testing on OT networks without creating operational problems, provided that the test itself is properly planned and tightly controlled.

- Remember: Threats to Operational Technology (OT) systems, can cause production stoppages, a decrease in product quality or even destruction of infrastructure

Social engineering (assessment on human resources)

In the last solar year the phishing/social engineering attacks are increased (+ 1.166% - Clusit report 2017).
In the last solar year, 77% of organizations have suffered a phishing attack, while 58% claim that this type of attack is on the rise. In addition, nearly 80% of malware attacks consist of phishing activities. Employees are the most vulnerable part of the company's security information and it is noted that most of the violations are attributed to employee behavior.

No technological solution can ever overcome the wrong behaviors (induced or voluntary), as no technology can withstand a social engineering attack (well structured and prepared).

Social engineering (assessment on human resources)

- The most important assessment is referring to **human resources**:
  - Social engineering
  - Awareness
  - Training
  - Security Culture
  - Policy
  - Digital investigation & forensic
  - Why we speack about it?
  - Because of **Behavior**

"I won a million dollars in an online lottery. Just as I was entering my social security number and other requested information, to transfer the money to my bank account, the computer froze."

Lloyd's Register LRQA

Improving performance, reducing risk

Social engineering (assessment on human resources)

- Over 75% of successful attacks have an internal base, a weakness of the system that is reflected in the weaknesses of the organization's security and security team

- Excessive confidence in ourselves technical skills, fear of confrontation with other entities, and focus on technology are enormous gaps in which it is possible to insert wedges capable of scrapping any organization. It is the human being, therefore, the weak element of the security chain.

- Computer security, with all its technology and novelty, can only be supportive

Conclusions: how does this fit in your company?

- This is 'a' race 'uninterrupted, you can not let' win 'to those who have won so far

- You do not need to see the whole staircase. Simply start to climb the first rung.
- (**Martin Luther King**)

- Luke Skywalker: Well, I'll try.
- Yoda: No! Do not try it. You either do or you do not. There is no try."
- (**Star Wars Movie**)

Thank you

Ilaria Savini
Senior Business Development Specialist
ilaria.savini@lr.org

Lloyd's Register
LRQA

Improving performance,
reducing risk