ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

# "STET" case study

Tiziano Sartori
STET S.p.A.

Konferenca za izzive vodenja, tveganj, varnosti in revizije IKT
Ljubljana, Oktober 2016

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

# Company profile and project introduction

# Company

The mission of Servizi Territoriali Est Trentino (East Trentino Services, acronym STET) is to distribute public services such as electric energy, gas and drinking water.

Furthermore, STET is an electric energy and thermic (warm and cold) energy producer and is a manager of public lighting systems.

It operates in a territory of 50 km radius thanks to specific contracts with local public entities  of small cities in eastern Trentino.

# Associates

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

- Municipality of Pergine Valsugana: 74,31%
- Municipality of Levico Terme: 18,97%
- Municipality of Caldonazzo: 4,63%
- Municipality of Tenna: 1,50%
- Municipality of Calceranica: 0,02%
- Municipality of Sant'Orsola Terme: 0,02%
- Municipality of Civezzano: 0,02%
- Municipality of Grigno: 0,02%
- Municipality of Novaledo: 0,01%

# Numbers

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

| | |
|---|---|
| End customers | 40.000 |
| Employers | 60 |
| Remote controlled systems | 150 |
| Annual profits | 12 mln € |
| Investements | 3 mln € |

# Needs and solutions

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

We checked the state of art of:

- organization management model;
- logic build of infrastractures;
- physic build of infrastractures;

In 2013 STET invested in specific metering activities with the following goals:

- company procedures and organization analysis by reading contextual documents;
- targeted people interviews;
- cyber attacks simulation;

# Results

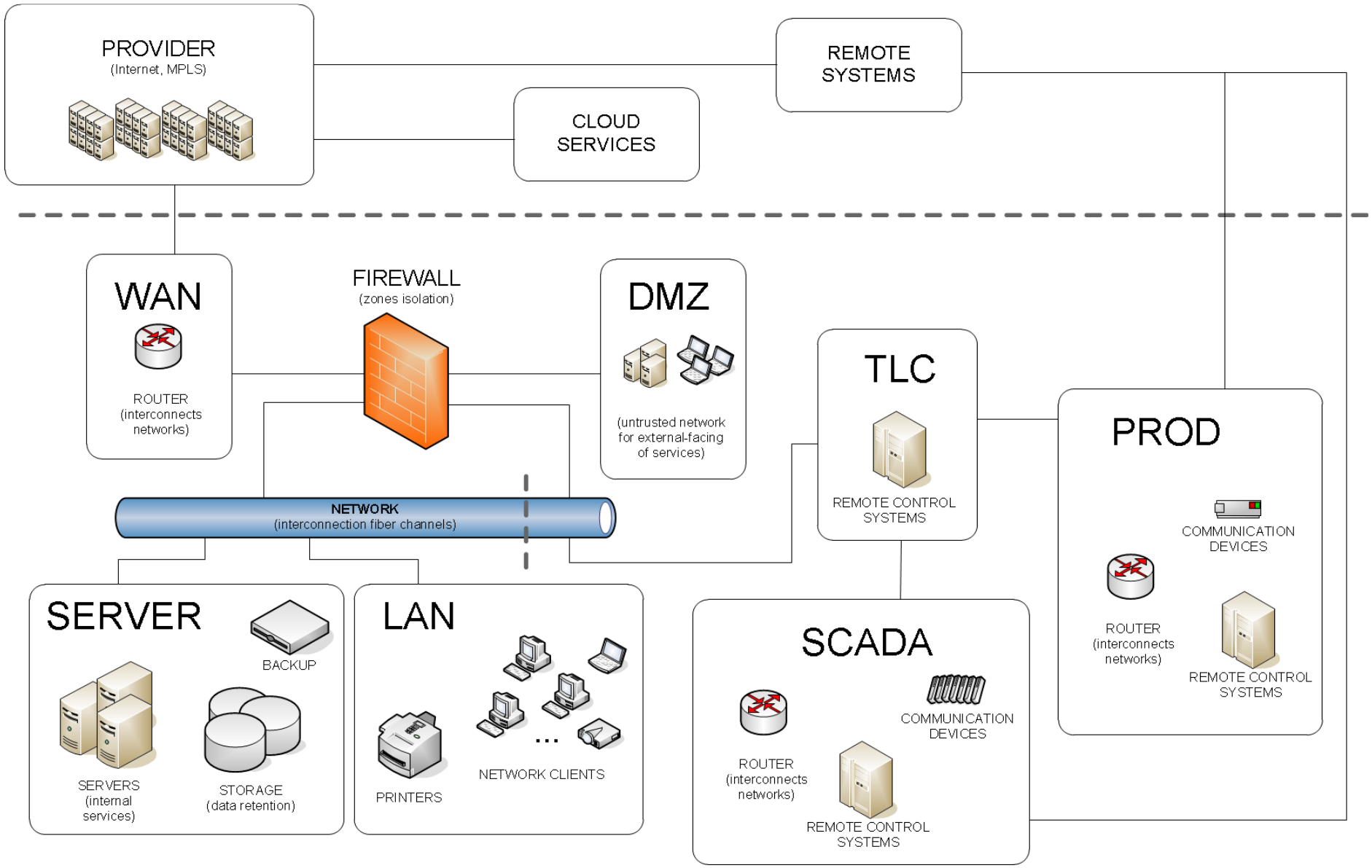
- This analysis highlighted how STET was already far above the security market standards, although improvements are still possible.
- An international standard report was produced highlighting the state of art. The repetition of this report will be shown enhancements in the future.
- Several projects have been started, showing good cost/benefits ratios.

ISACA®
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

# ICT infrastructure and security analysis planning

# ICT infrastructure

ISACA
Zaupanje v informacijske sisteme in koristi od njih
Slovenski odsek



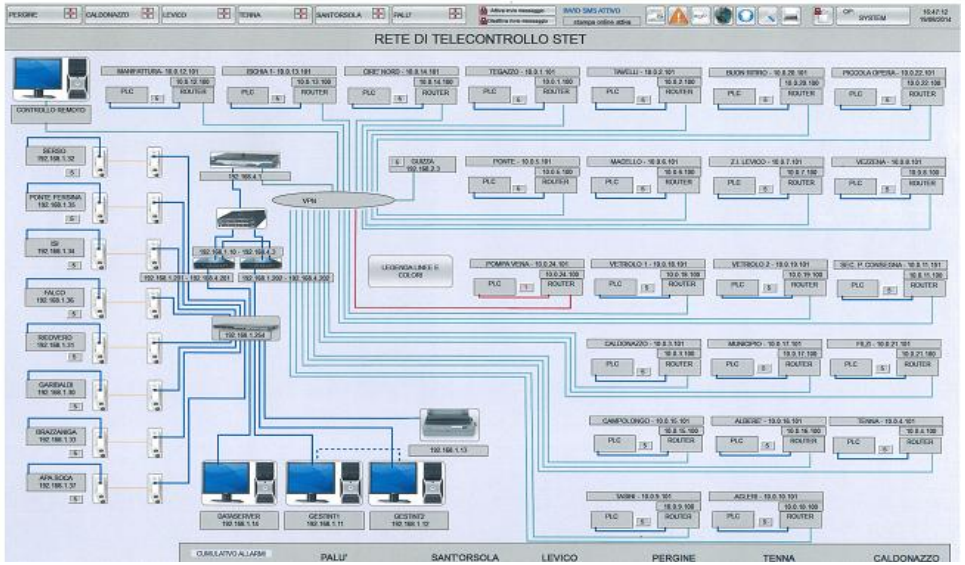
# SCADA (1/3)

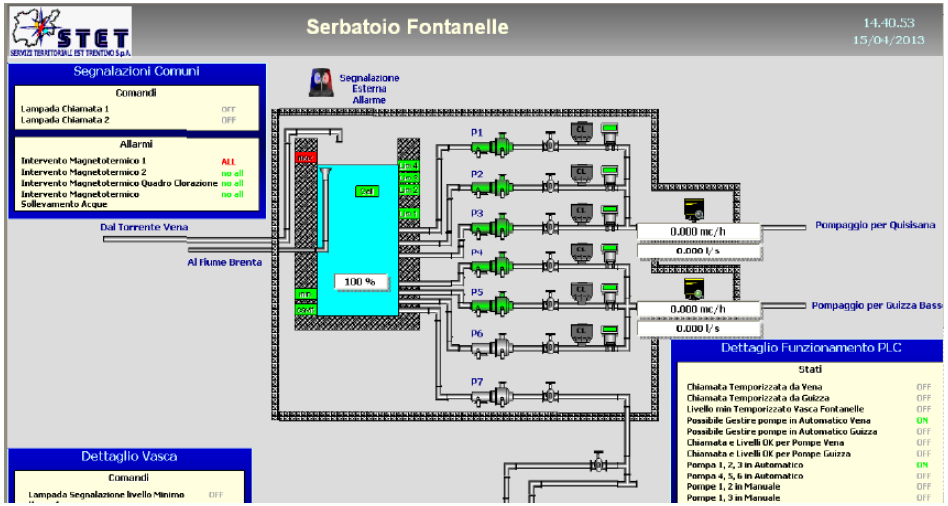
ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

- The STET remote control center (called CTC) is located in the company headquarter;
- The systems are located in the suburbs, connected with different communication technologies:
  - 3G/GPRS
  - DSL
  - Radio bridges
  - Fiber channels
- All communications happen through VPN tunnels, in some cases managed by TLC providers.

# SCADA (2/3)

ISACA
Zaupanje v informacijske sisteme in koristi od njih
Slovenski odsek



# SCADA (3/3)

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

These are the types of managed systems:

- electrical substations;
- pumping systems;
- tanks for water storage;
- gas distribution substations;
- energy generating stations;
- alarm and video surveillance systems;

# Project steps

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

1. Collection and analysation of oral and written information
2. Check of collected information and review of a starting document
3. Vulnerability Assessment execution in order to identify the systems vulnerabilities or misconfigurations

# Check methods

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

- Logical and physical security in the control center and in branch offices (building perimeter, access doors, locks, unlocking passwords, etc.).
- Security inspections of operative systems and communication media through cyber attacks simulation, software/firmware version checks and network zones isolation analysis of all systems.

ISACA®
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

# Advice examples

Strenght and weakness points

# Documents

ISACA
Zaupanje v informacijske sisteme in koristi od njih
Slovenski odsek

From 2003 to 2010 the Italian law required to write and edit a specific document called DPS with the purpose of describing company security policies.

After 2010, STET keeps updating this document with the aim of having an updated description of the IT infrastracture's state of art. This "best practice" places STET over market standards.

At the present time, further information have been added, such as:

- more detailed network topologies;
- list of employers of IT and SCADA departments;
- guests management procedures;
- end user manuals;

The revision now is organized according to ISO 9001 standards.

# Remote support (1/2)

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

Remote support methods were one of the STET procedures critical point. Too many suppliers, each with its own type of assistance technologies caused a high number of uncontrolled access doors to the systems, increasing exposition to attacks.

Today, every supplier uses the same software technology, regulated by specific policies. The accesses can now be organized and monitorated (people who login, date and time login/logout events, destinations filtering, etc…) directly in the core firewall systems.

# Remote support (2/2)

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

…right from web:

Abbadia San Salvatore, electric substation cracked.

http://altracitta.org/2014/08/26/abbadia-san-salvatore-hackerata-la-centrale-elettrica-su-twitter-il-pannello-di-controllo/

# Devices firmware

ISACA
Zaupanje v informacijske sisteme in koristi od njih
Slovenski odsek

During systems test phase some software vulnerabilities were detected. These weaknesses exist because PLC devices work fine for the systems orchestration but they are not efficient for networking communications.

Targeted tests with specific exploiting software toolkits reveal how some attacks can bring to isolation of the systems.

The only way to protect these systems is constantly check the devices firmware, update them on pre-production infrastractures before consolidating them in production environments.

These procedures cannot always be convenient. That's why your PLC vendor choice can make the difference. Whether possible, STET has tested and updated its devices to newer firmware versions.

# IT systems isolation

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

The isolation of STET network zones ranks the company over the market standards.

In the future there will be no more single physical zones. They will be replaced by a big logical interconnected zone.

The replacement of some network devices allowed to follow this path, permitting a further separation of the subnets with “1-site:1-subnet” logic.

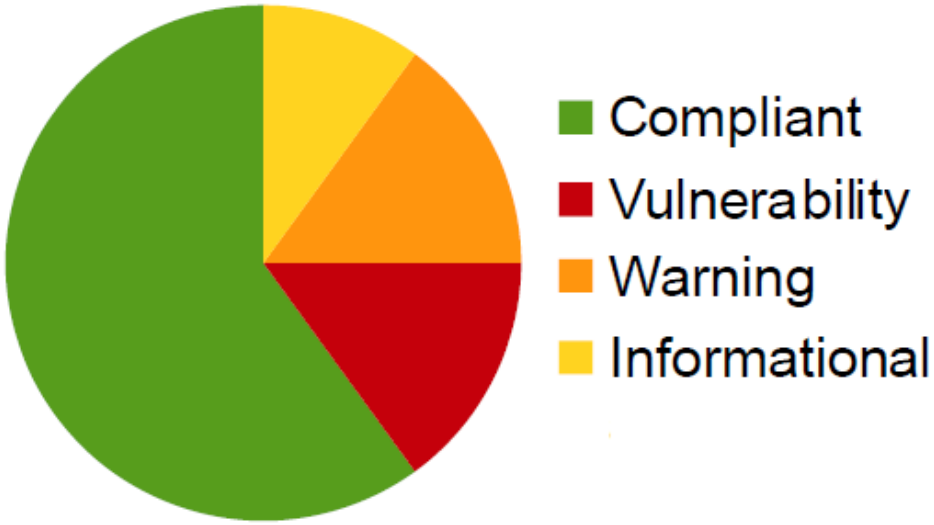
# Others

- Wireless (802.11) attacks and disturbs
- Network devices redundancy (clustering)
- Patching (guest OS, network devices)
- DR e BC
- Conf and Incident management (ticketing, tracking)
- ….

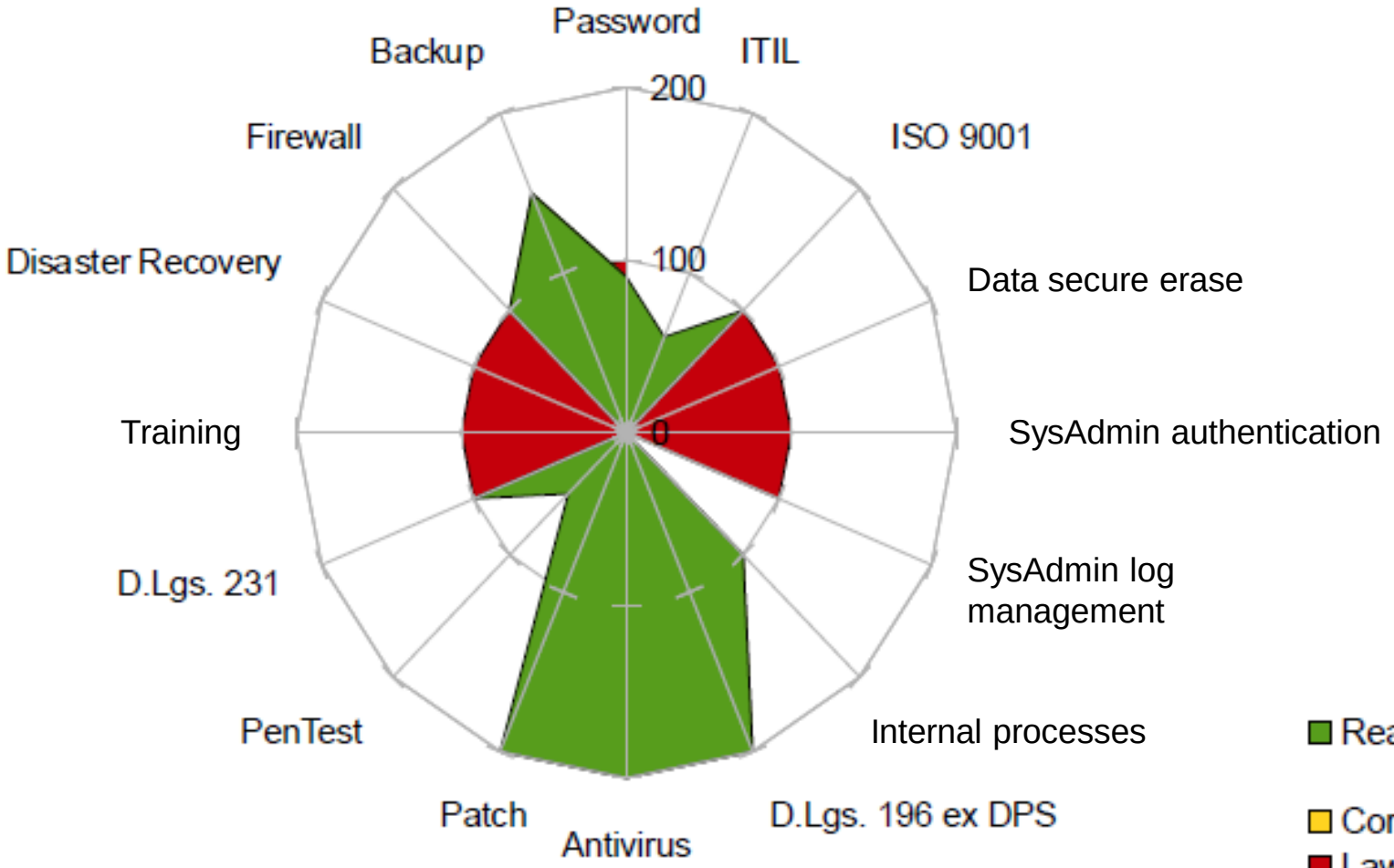
# Results

# Detected risks

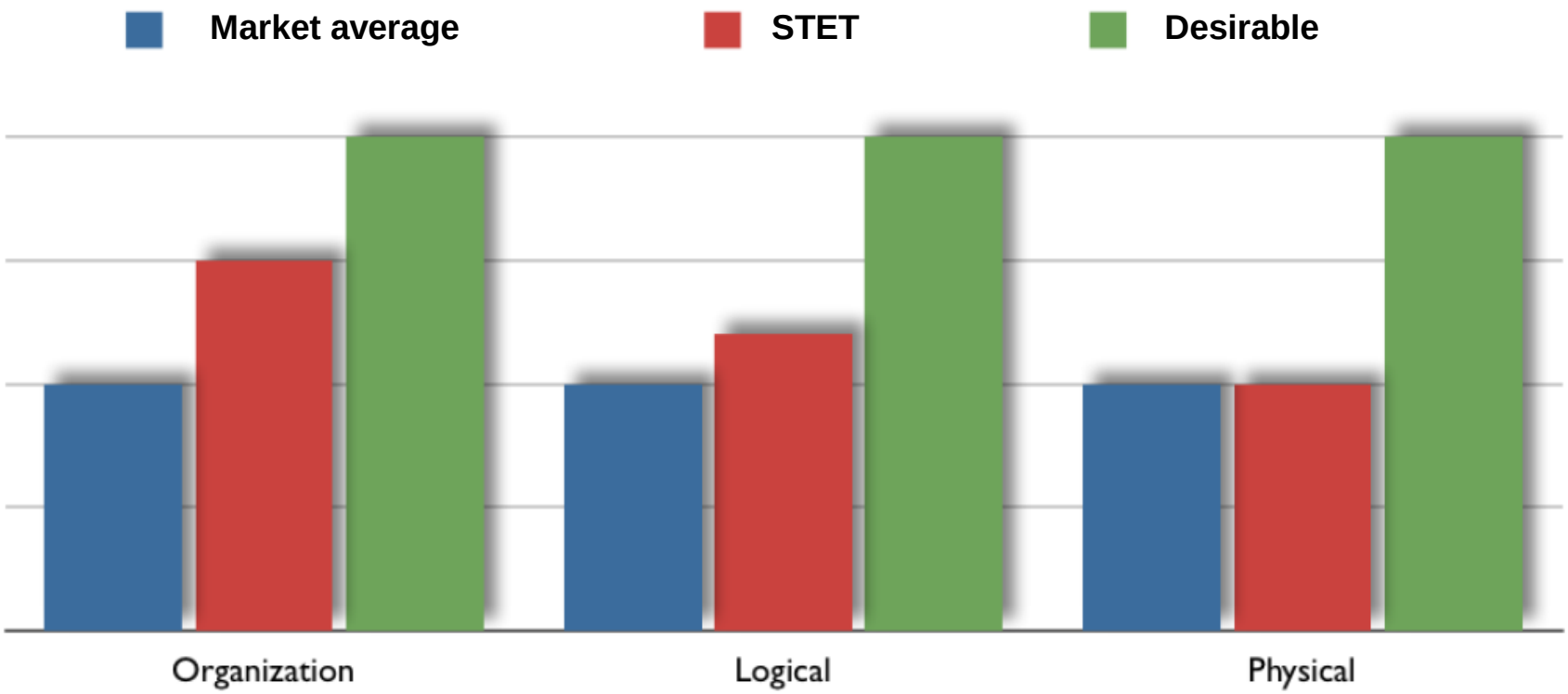
| | |
|---|---|
| **Compliant** | 60 |
| **Vulnerability** | 15 |
| **Warning** | 15 |
| **Informational** | 10 |



# Non-compliance



# Current and desirable rank



# Remediation matrix (example)

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

| Remediation advice | Security type | Gravity (1-3) | Urgency (1-3) | Economic impact (1-3) | Organizational impact (1-3) |
|---|---|---|---|---|---|
| #1 | Organization | 1 | 1 | 0 | 1 |
| #2 | Organization | 3 | 3 | 2 | 2 |
| #3 | Logical | 2 | 3 | 2 | 2 |
| #4 | Physical | 3 | 3 | 2 | 1 |
| … | | | | | |

# Attack Surface Security Metrics

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

Actual Security: 70,04 ravs

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES


OSSTMM version 3.0

# Specific site analysis (example 1/2)

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

***Legenda***

| | | |
|---|---|---|
| **Impatto** | Vulnerabilities | Problema che permette di<br>• bloccare l'accesso agli utenti autorizzati<br>• ottenere l'accesso ad asset riservati<br>• nascondere la propria presenza a persone non autorizzate |
| | Weaknesses | Problema che riduce o annulla l'efficacia dei controlli di classe A |
| | Concerns | Problema che riduce o annulla l'efficacia dei controlli di classe B |
| | Exposure | Problema che permette la visibilità diretta o indiretta di asset, senza che questo sia previsto o motivato |
| | Anomalies | Elemento incognito che non è stato controllato |
| **Likehood** | Alto<br>Medio<br>Basso | Probabilità che questa anomalia venga sfruttata.<br>es. alta per programmi diffusi affetti da vulnerabilità conosciute e di cui sia disponibile un exploit funzionante |
| **Fix Effort** | Alto<br>Medio<br>Basso | Valutazione dell'effort economico e/o organizzativo per mettere in sicurezza il problema riscontrato; valore basato anche sul budget IT del cliente |

# Specific site analysis (example 2/2)

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

| Host | Vulnerabilities | Weaknesses | Concerns | Exposures | Anomalies | Compromesso |
|---|---|---|---|---|---|---|
| 192.168.5.112 | 1 | 0 | 0 | 0 | 0 | SI |

| [redacted] PLC consente esecuzione comandi senza autenticazione | | |
|---|---|---|
| **Impatto** | **Likehood** | **Fix Effort** |
| Vulnerability | Medio | Alto |
| | | |
| **Descrizione** | | |
| Il PLC contiene una vulnerabilità nota che permette l'esecuzione di comandi senza autenticazione. Su internet è disponibile un exploit dimostrativo che permette l'esecuzione di comandi di spegnimento del PLC. | | |
| **Host Affetti** | 192.168.5.102 | |
| **Soluzione** | | |
| Aggiornare il firmware | | |

# Conclusions

# Conclusions

ISACA
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

STET's short and mid term goal is to keep investing in ICT security.

Another Vulnerability Assessment and Penetration Test has been scheduled in order to hightlight the differences between the past and the future.

A project of a new Disaster Recovery Site was planned, far from headquarter, considering possible natural disasters (e.g.: earthquakes, fire, etc…).

# References



- http://www.stetspa.it
- https://en.wikipedia.org/wiki/Critical_infrastructure
- http://www.isecom.org/research/osstmm.html

ISACA®
Zaupanje v informacijske sisteme in korist od njih
Slovenski odsek

# Thanks for your attention!

Konferenca za izzive vodenja, tveganj, varnosti in revizije IKT

Ljubljana, Oktober 2016