Cybersecurity e Vulnerabilità dei Sistemi SCADA

Settembre 2011 – Workshop Sicurezza Energy & Utilities

Andrea Zapparoli Manzoni

Il Clusit

Associazione "no profit" fondata nel 2000
presso l'Università degli Studi di Milano,
Dipartimento di Informatica e Comunicazione

Le priorità del Clusit per il 2011 e 2012:

- **Formazione specialistica**: Seminari CLUSIT (a Milano e Roma)
- **Certificazioni professionali**: corsi ed esami CISSP e CSSLP (MI e RM)
- **ROSI**: un metodo per valutare il ritorno dell'investimento in sicurezza informatica
- **Security Summit:** le Conferenze specialistiche: (Milano, Roma e Verona)
- **Ricerca e studio**: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi
- **Progetti Clusit** per piccole e microimprese: per aiutarle a gestire il rischio IT, in collaborazione con le associazioni imprenditoriali locali
- **Canale Clusit** su YouTube: la sicurezza ICT in video pillole
- **Progetto Scuole**: Formazione sul territorio
- **Rapporti Clusit**: Rapporto annuale sugli eventi dannosi (Cybercrime e incidenti informatici) in Italia; analisi del mercato italiano dell'ICT Security; analisi sul mercato del lavoro.

Il Relatore

Andrea Zapparoli Manzoni nasce nel 1968 a Milano, frequenta il Liceo Classico, si laurea in Scienze Politiche e consegue un dottorato in Relazioni Internazionali presso l'Università di Berkeley (USA).

- Inizia l'attività lavorativa nel 1995, e si interessa attivamente di **ICT Security** dal 1997, con particolare riferimento alle tematiche **GRC** (Governance, Risk e Compliance).
- Negli anni si occupa di **IDM, IAM, DLP, Anti Frode, Security Intelligence, Forensics, Cyberwarfare, Vulnerability Assessment e Management** in contesti Enterprise, Industriali, PA Centrale e Gov-Mil.
- Scrive **articoli e saggi** su tematiche di sicurezza, e segue con grande attenzione tutte le evoluzioni della cybersecurity a livello internazionale.
- In qualità di **trusted advisor** collabora con Enti ed Istituzioni, nazionali ed internazionali.
- Contribuisce alle attività di **Clusit** partecipando a convegni, realizzando documenti (ROSI, DLP, SCADA) e diffondendo la cultura della sicurezza informatica in Italia.
- Oltre a collaborare con numerose aziende italiane ed estere, è **fondatore e CEO de iDialoghi**, società specializzata nella realizzazione di soluzioni di Information Security avanzate / non convenzionali, incluso l'ambito SCADA.

1. SCADA: Evoluzione delle Minacce

“SCADA Security Today: Where Enterprise Security Was 10 Years Ago”.

“Technology has blurred the line between the physical machine and the electronic machine driving our infrastructure”.

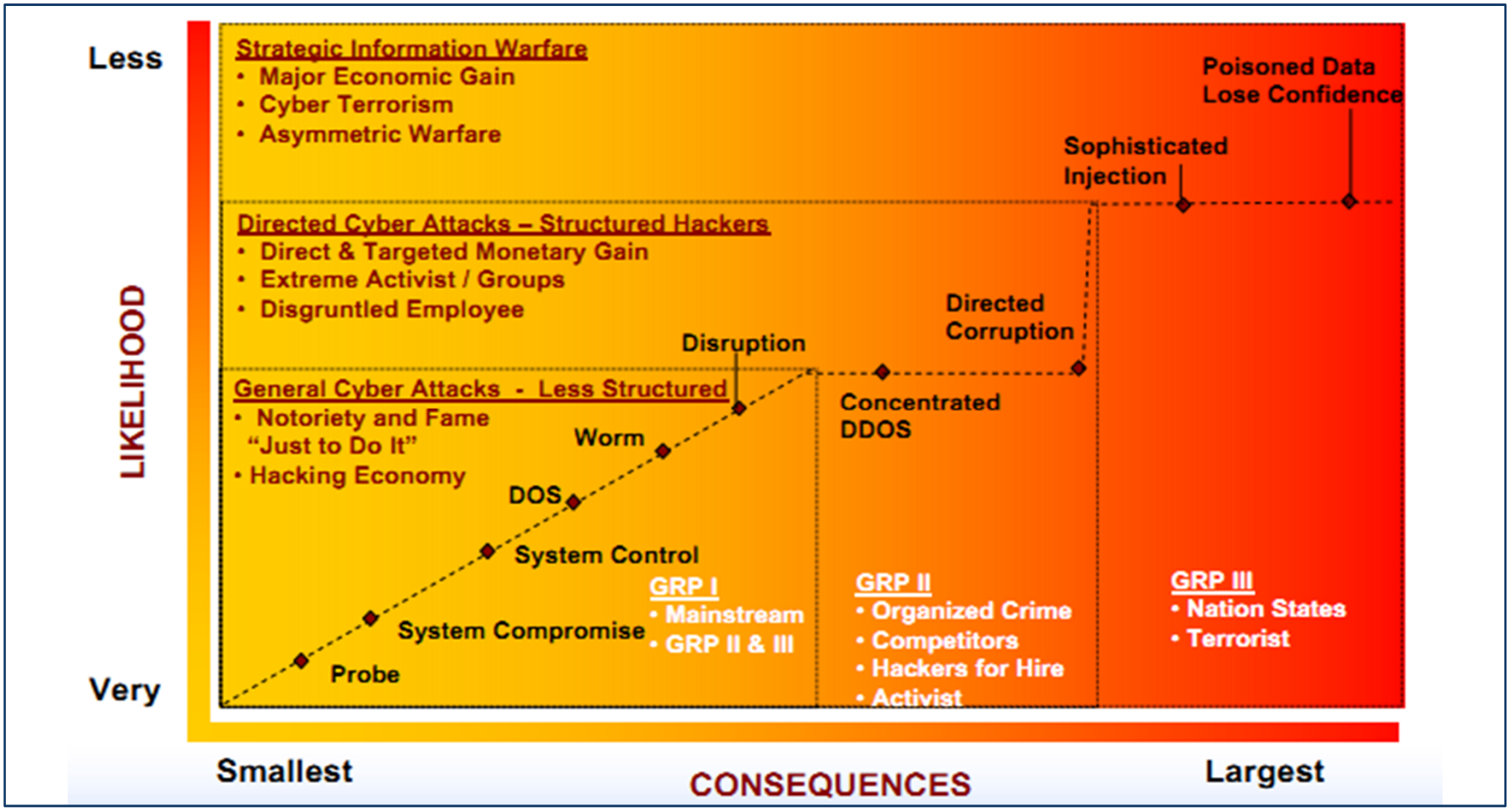
“The present state of security for SCADA is not commensurate with the threat or potential consequences”.

Avvenimenti recenti:

- Cyber **Hacktivism**: Anonymous, attivismo politico (nazionalisti, ecologisti, antagonisti in genere)
- Cyber **Sabotage**: StuxNet (oltre alle sue evoluzioni e conseguenze), Terrorismo
- Cyber **Espionage**: Op. “Byzantine X”, “Aurora”, “Night Dragon”, “Shady RAT”, “Black Tulip”, etc
- Cyber **Warfare**: I principali Paesi hanno pubblicamente dichiarato di avere acquisito capacità in ambito **cyberwar**, ed hanno istituito **Comandi** ed **Unità** militari ad hoc. In questo nuovo dominio, la maggior parte dei target **sono infrastrutture critiche**, per lo più governate con sistemi SCADA.
- Crescente interesse da parte della **comunità hacker**: più vulnerabilità disclosed nel 1Q 2011 che in tutto il 2010, ed il trend sta accelerando. Ben pochi sono White Hats!

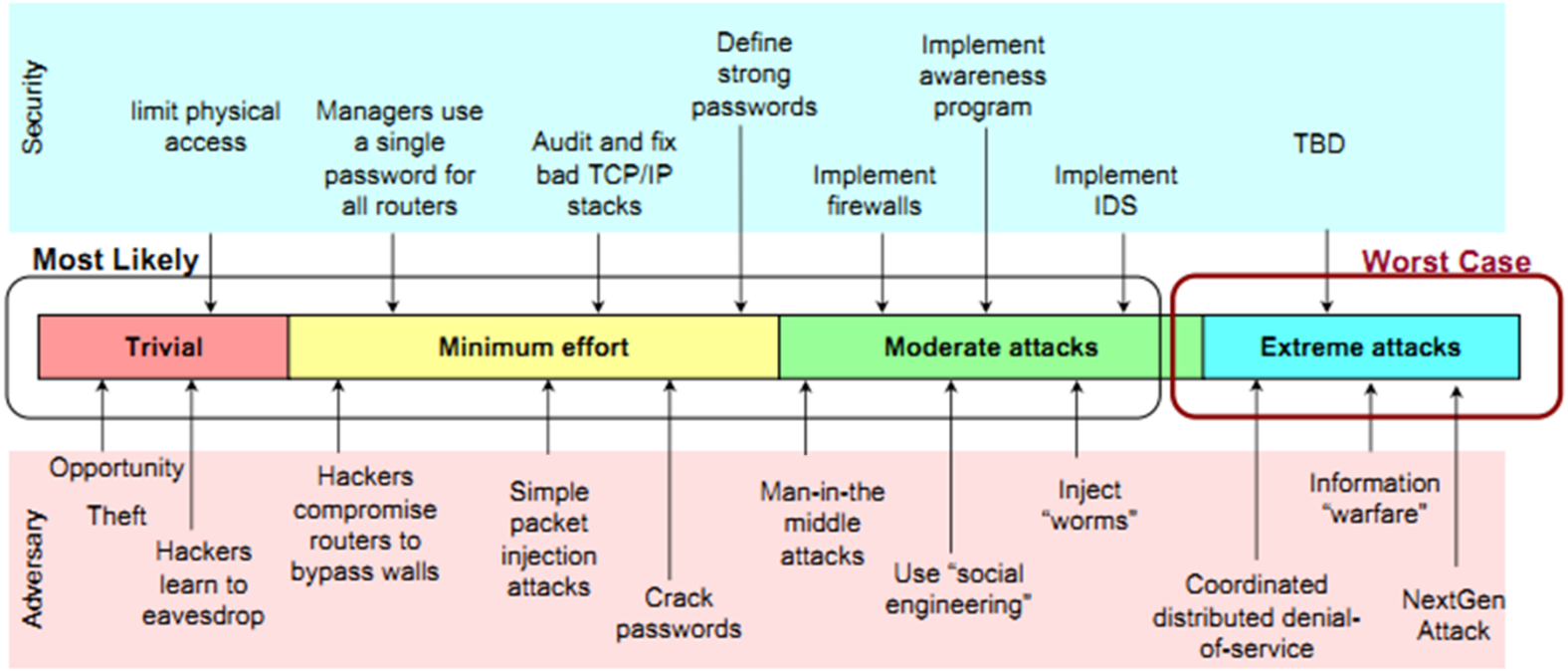
2. Rischi più gravi e più probabili

Le **minacce** stanno aumentando in termini di **gravità** e di **probabilità** di accadimento (la curva si sta appiattendo). L'avvento di concreti scenari di **Cybersabotage** e di **Cyberwar** sta elevando fortemente i rischi di **incidenti gravi**.



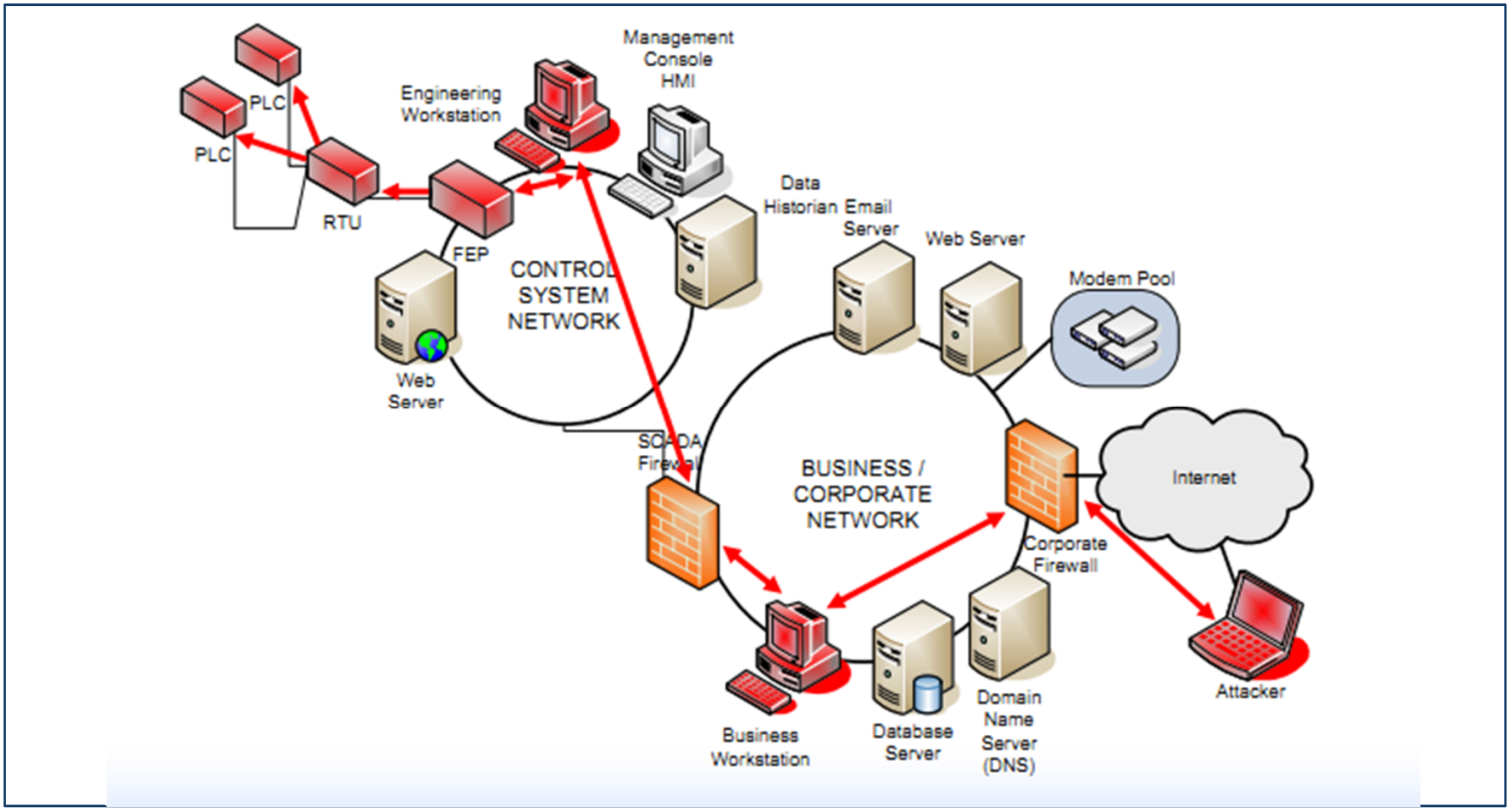
3. Crescente complessità delle contromisure

Per tutti i motivi sopra esposti, invece che ridursi, la **finestra di vulnerabilità** si sta **allargando**. La crescente **apertura** delle reti SCADA verso l'**esterno** e verso le **reti di business** rende le contromisure sempre più **complesse**.



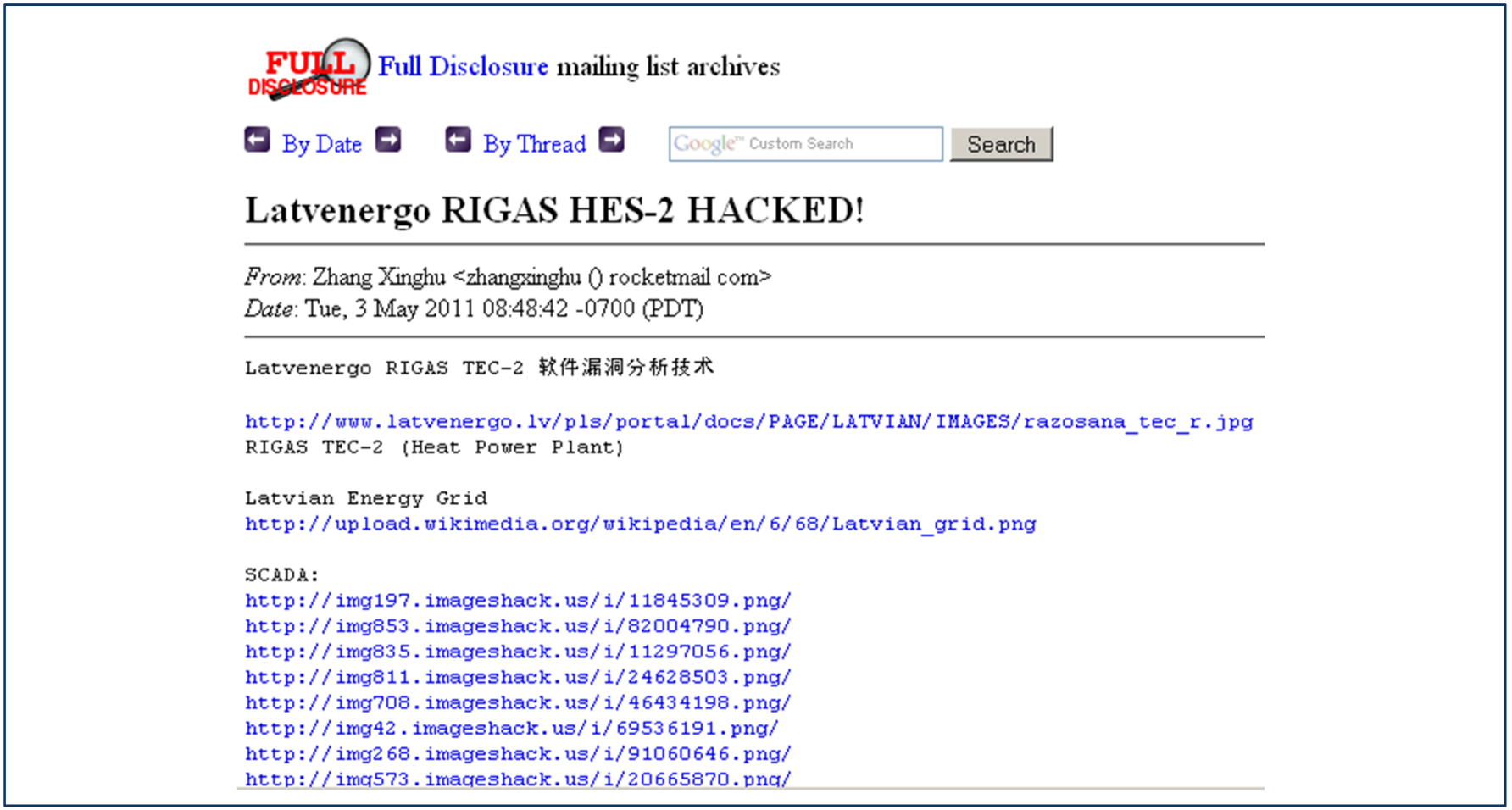
4. Tipologie di attacchi a Sistemi SCADA (1)

StuxNet a parte, che rappresenta un caso particolare, sempre più spesso si osservano attacchi condotti impiantando **APT (Advanced Persistent Threats)** nel **business/corporate network**, e **da lì** raggiungendo il network dei sistemi di controllo SCADA.



5. Tipologie di attacchi a Sistemi SCADA (2)

Un altro genere di attacco, sempre più comune, viene condotto compromettendo le interfacce **Web based** di sistemi di gestione SCADA esposte su **Internet**… Spesso individuate semplicemente tramite **Google**! Esiste addirittura un search engine, chiamato **Shodan,** che indicizza **solo** sistemi SCADA insicuri esposti sul Web.



Full Disclosure mailing list archives

By Date By Thread Google™ Custom Search Search

Latvenergo RIGAS HES-2 HACKED!

From: Zhang Xinghu <zhangxinghu () rocketmail com>
Date: Tue, 3 May 2011 08:48:42 -0700 (PDT)

Latvenergo RIGAS TEC-2 软件漏洞分析技术

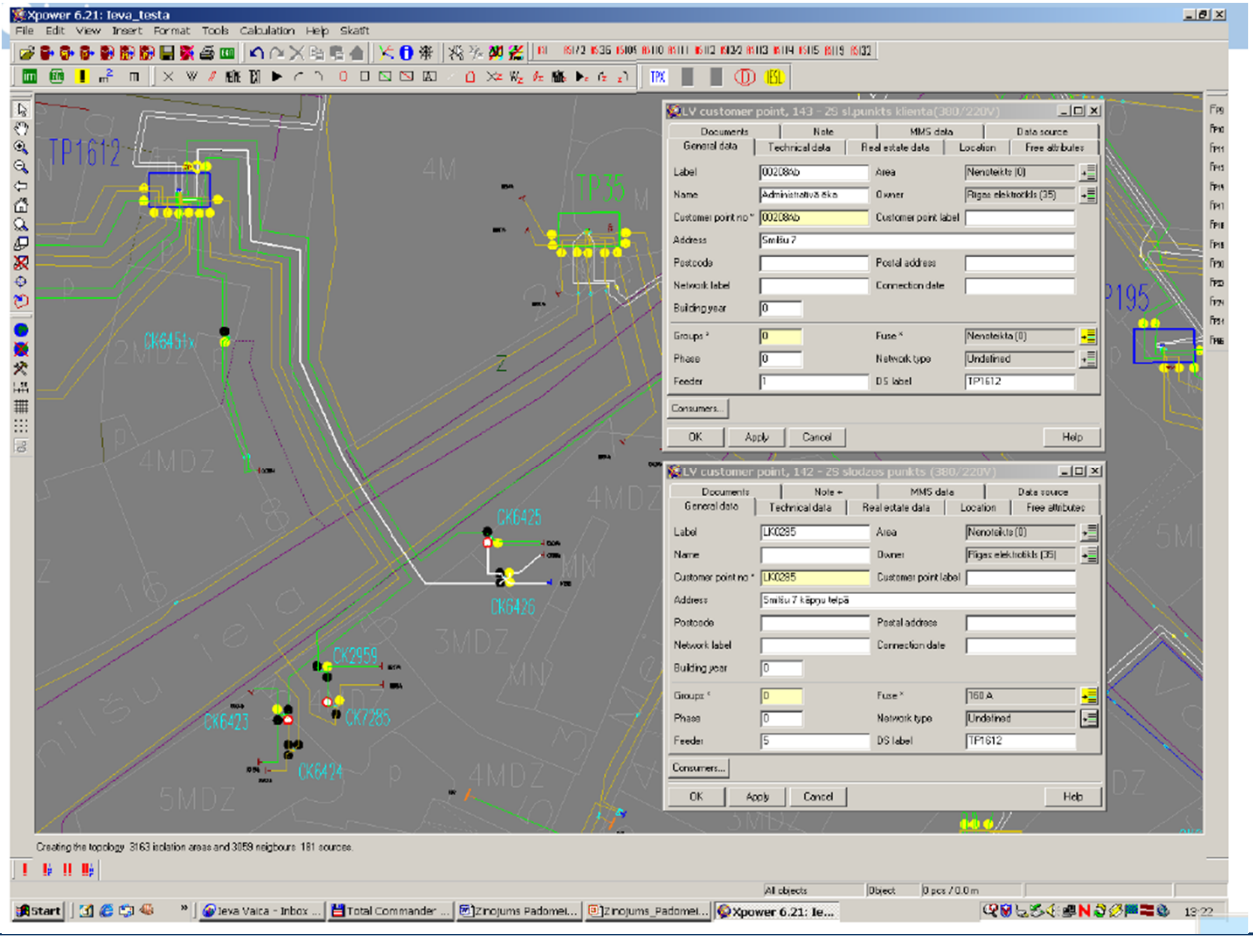
http://www.latvenergo.lv/pls/portal/docs/PAGE/LATVIAN/IMAGES/razosana_tec_r.jpg
RIGAS TEC-2 (Heat Power Plant)

Latvian Energy Grid
http://upload.wikimedia.org/wikipedia/en/6/68/Latvian_grid.png

SCADA:
http://img197.imageshack.us/i/11845309.png/
http://img853.imageshack.us/i/82004790.png/
http://img835.imageshack.us/i/11297056.png/
http://img811.imageshack.us/i/24628503.png/
http://img708.imageshack.us/i/46434198.png/
http://img42.imageshack.us/i/69536191.png/
http://img268.imageshack.us/i/91060646.png/
http://img573.imageshack.us/i/20665870.png/

5. Tipologie di attacchi a Sistemi SCADA (2)

Un altro genere di attacco, sempre più comune, viene condotto compromettendo le interfacce **Web based** di sistemi di gestione SCADA esposte su **Internet**… Spesso individuate semplicemente tramite **Google**! Esiste addirittura un search engine, chiamato **Shodan,** che indicizza **solo** sistemi SCADA insicuri esposti sul Web.



6. Un modello per Mitigation e Remediation

Mitigation e **remediation** sono possibili solo applicando un modello di sicurezza **multi-layer (defense in depth)**, ovvero implementando **contestualmente** una serie di layers di difesa (organizzativi, educativi, logici e fisici) su tutta la "filiera" che costituisce un ambiente SCADA / DCS ed il suo **contorno**.

1 Perimeter Controls –
Internet & Corporate Perimeter

2 Access Control,
People, Policies

Cyber Control

3 Network Architecture Components

4 Operating Systems

5 Host Security

6 Application Security

7 Core Operational Services

7. Fondamenti della SCADA Cybersecurity

Negli ultimi anni si è consolidato un **consenso** crescente in merito a quali siano i **9 elementi** "core" della SCADA Security, interpretati alla luce di un necessario processo di **Risk Management** da un lato, e di **Vulnerability Management** dall'altro. L'insieme di questi 9 macro-elementi **costituisce la base** della SCADA Cybersecurity.

- Monitoring and Investigative Processes
  - Monitoring & Logging
  - Forensics & Investigations
  - Threat Analysis & Assessment
- Risk and Vulnerability Management Processes
  - Risk Management
  - Vulnerability Management
  - Secure Development Life Cycle
- Response and Continuity Processes
  - Business Continuity Planning
  - Crisis Management
  - Incident Response

8. Grazie!