La governance della Cyber Security nei sistemi ICS/SCADA

DXC Technology

Giornata di studio ISA/AIS

October 25, 2018

Your speaker today

Leonardo Nobile

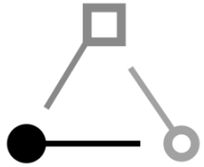
DXC Technology - Security Principal

South EMEA

- Broad experience (23+ years) in Big Four, Technology companies and Financial Intermediary
- Extensive knowledge of IT Security, IT Governance, IT Compliance and IT Risk Management techniques and methodologies
- Proven experience in Cobit use and APMG Accredited Cobit5 trainer
- Certified in: Cobit 5 Foundation, APMG Accredited Cobit 5 Trainer, CISA, CISM, ITIL V3 Foundation, Lead Auditor ISO27001, Lead Auditor ISO22301, CDP Privacy Officer (TUV)
- Current experience in DXC Technology as Security Principal

I sistemi ICS / SCADA

La sicurezza nelle organizzazioni è sotto pressione



IT departments feel the squeeze but…

budgets are under pressure and security is now a board-level issue

The innovative adversary

is increasingly sophisticated and, on average, goes undetected for 99 days[1]

Security operations

need maturity, speed & scale to move beyond real-time threat monitoring

Next generation threats

such as ransomware or file-less, memory-based malware makes it difficult to stay secure

Regulatory pressures

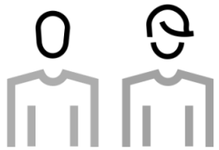
grow for industry and geography compliance requirements such as GDPR

Widening skills gap

makes it hard to attract, train, and retain security professionals, yet the demand for security talent is expected to increase by 53% in 2017[2]

Device, cloud explosion

is causing significant increases in the enterprise threat surface



People are weakest link

and require awareness and training to protect against the 80% of attacks that target user access[3]

Sources:1: Mandiant M-Trends 2017 Report; 2: US Bureau of Labor Statistics, 3: CyberArk Security Report 2015

Il ruolo dei sistemi di controllo industriale

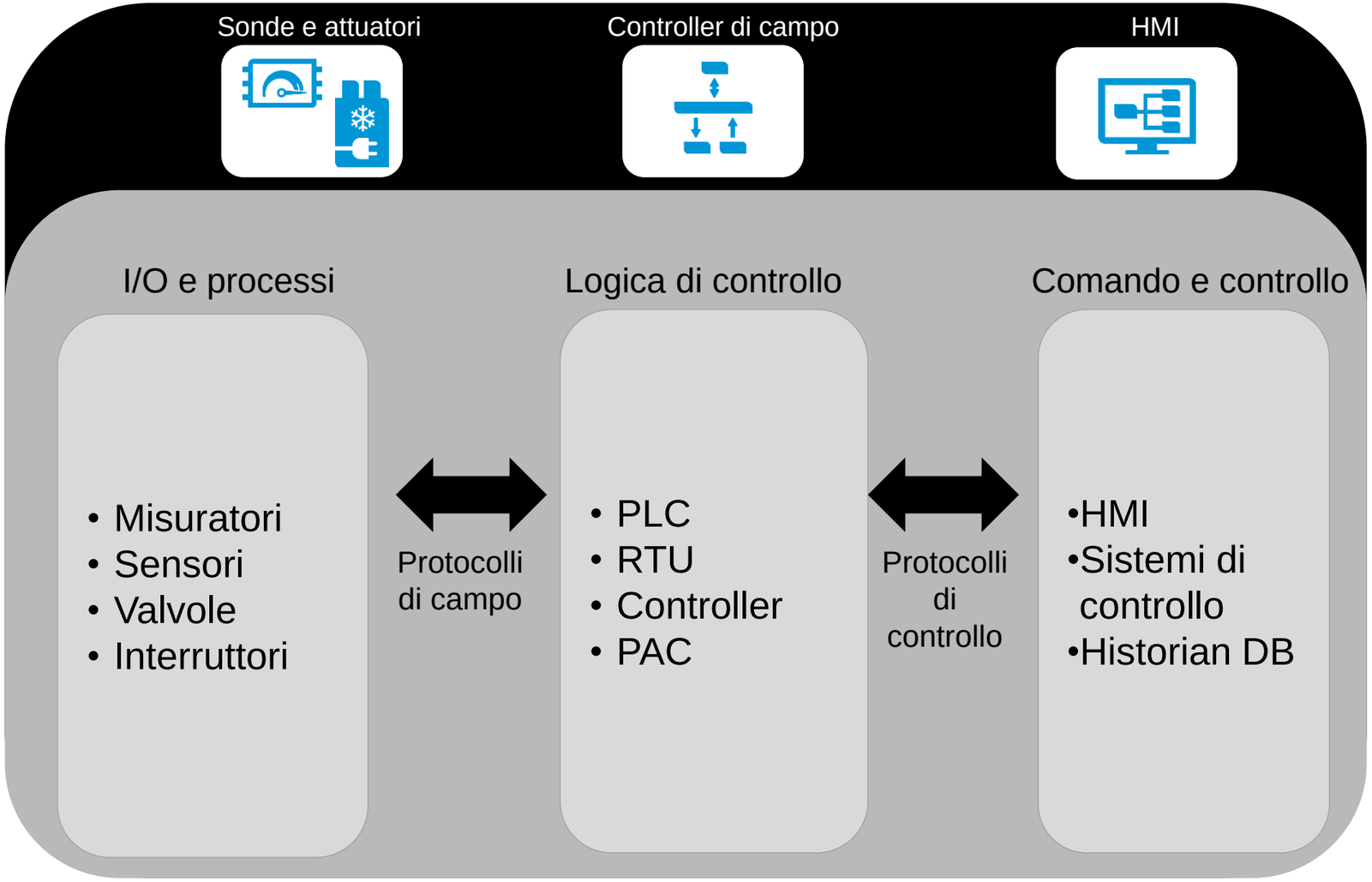
I sistemi automatici di controllo industriale permettono a numerosi settori di operare con adeguati livelli di affidabilità e sicurezza

- Chimica
- Commercio e distribuzione
- Manifattura
- Energia
- Pharma
- Acquedotti
- Trattamento rifiuti
- Telecomunicazioni
- Trasporti
- Poste e spedizioni

Architettura e caratteristiche delle reti ICS/SCADA

Il termine Sistema di Controllo Industriale (ICS – Industrial Control System) fa riferimento a differenti sistemi, fra i quali:

- SCADA (Supervisory Control and Data Acquisition)
- DCS (Distributed Control System)
- PCS (Process Control System)
- EMS (Energy Management System)
- AS (Automation System)
- SIS (Safety instrumented system)



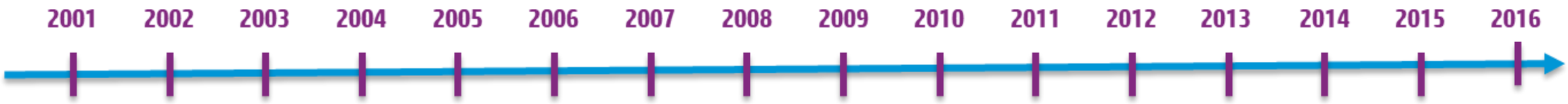
Sicurezza ambienti IT vs ICS

A causa delle differenti finalità di sistemi ICS e Metering, rispetto ai sistemi IT, l'approccio alla sicurezza deve essere adattato

Elemento	IT standard	ICS
Protezioni degli endpoint	Ampiamente utilizzato	Impiego limitato, e con cautele
Tempo di vita dei sistemi	3-5 anni	10-15 anni ed oltre
Outsourcing	Pratica accettata	Uso limitato
Patching	Regolare	Lento – può richiedere la preventiva approvazione e testing del fornitore tecnologico
Change management	Regolare	Richiede tempi lunghi
Ritardi elaborativi	Possono spesso essere tollerati	Possono avere impatti anche gravi
Security Skills & Awareness	Buona	Limitata
Security Testing	Sempre più diffuso	Impiego limitato, e con cautele
Physical Security	Presidiata	Buona, ma possono esistere sistemi non presidiati
Profilo di rischio	Gestione di dati, confidenzialità ed integrità fattori centrali	Controllo dei processi fisici, sicurezza (safety) il principale elemento di preoccupazione

I profili di rischio per i sistemi ICS/SCADA

I sistemi SCADA stanno diventando un obiettivo strategico?



2001 – Porto di Houston. System crash

2003 – Slammer Worm. Controllo di volo, ATM, 911, Sistema di monitoraggio centrale nucleare

2003 - 2004 – Titan Rain. Attacchi contro Installazioni militari

2007 – Tehama Canal Auth. Ex dipendente installa SW non autorizzatosu un computer per il controllo idirico

2009 – Attacco alla rete di distribuzione elettrica USA. Attacco individuato dall'FBI

2009 – 2010 – Operazione aurora. Furto di proprietà intellettuale. Fra i target, aziende di sicurezza

2010 – **Stuxnet**

2010 – NATO inizia la serie di esercizi Locked Shield»

2011 – Nitro. Attacco contro industrie chimiche, utilizzando un trojan acquistabile sul mercato nero

2012 – Shamon. Malware disabilita centinaia di computer di Saudi Aramco

2012 – Flame. Attacco contro sistemi Iraniani per raccogliere informazioni sul programma nucleare

2012 – Attacco contro le reti di utilities mirante al furto di credenziali. Identificato da ICS-CERT

2013 – US ICS-CERT riporta oltre 200 attacchi ad infrastrutture critiche (53% energy)

2013 – NATO lancia una massiccia esercitazione di cyberdefence: Cyber coalition 2013

2014 – Havex. Trojan capace di infettare sistemi ICS di 3 vendor.

2015 – NATO Locked Shield focalizzato su sistemi ICS/SCADA

I principali rischi dei sistemi ICS/SCADA

Frodi / Sabotaggi

Rischio di frodi/sabotaggi ai danni dell'azienda

Indisponibilità del servizio

Mancata disponibilità di servizi con impatti sull'operatività di risorse, utenti business e di alta direzione o su un numero significativo di clienti

Alterazione / Perdita di dati

Alterazione/perdita di dati di business sulla clientela

Non conformità

Complessità della normativa

Mancanza di uno schema di certificazione

Produttori di Meter ancora non pienamente allineati alla norma Confidenzialità dei dati

Reputazione

Impatti su dati e servizi visibili alla opinione pubblica o che compromettono la reputazione dell'azienda e il grado di fiducia della clientela

Il contesto regolamentare

La pressione regolamentare in ambito ICS/SCADA

Stati Uniti

- **NIST CSF**- Framework for Improving Critical Infrastructure Cybersecurity
- **NIST 800-82** Rev 2 (2015)- Guide to Industrial Control Systems (ICS) Security
- **NERC North America Electric Reliability Corporation: CIP 1300** Critical Infrastructure Protection
- **ES-C2M2** – Electricity Subsector - Cybersecurity Capability Maturity Model (Department of Energy - DoE)

Comunità Europea

- **ENISA** - Protecting Industrial Control Systems - Recommendations for Europe and Member States
- Good practice guide for CERTs in the area of Industrial Control Systems
- **EU Cybersecurity Strategy**
- **EU NIS Directive** - Network and Information Security (EU2016/1148)

Italia

- **EU NIS Directive** – Recepita in Italia con il DPCM 16/5/2017 e in vigore dal 26/6/2017
- **Quadro Strategico Nazionale per la Sicurezza dello spazio cibernetico** (2013)
- DPCM 13 aprile 2017 (DPCM Gentiloni)
- **Piano Nazionale per la protezione Cibernetica e la Sicurezza Informatica** (2017)
- **SEN:** Piano di ricerca nel settore elettrico + collaborazione a livello internazionale + PPP

Global Best Practices E&U

- **ISO 27019:2017** - Information technology -- Security techniques -- Information security controls for the energy utility industry
- **ISA/IEC 62443** – Security for industrial automation and control systems
- **IEC 62351:2018** - Power systems management and associated information exchange - Data and communications security
- **IEC 61513:2011** - Nuclear power plants. Instrumentation and control important to safety - General requirements for systems

Case Study
Assessment Sicurezza SCADA e Smart Metering

Approccio di Security Governance di riferimento

- Senior Management commitment
- Staff awareness
- Vendors

- Risk Scenarios
- Risk Methodology
- Scope (internal vs outsourcer)
- Asset Inventory
- Identify Risk Items
- Analysis Methodology

- Perform analysis
- Vendor documentation
- Security Laboratory
- Identify Vulnerabilities
- Define an action plan to mitigate risks
- Activate initiatives
- Obtain ICS/SCADA Security Readiness

- Security Specification for Purchasing
- Continuous Vendor Management
- Documentation
- Appliance Tests for new or existing products
- Threat Intelligence and vulnerability management

Punti di attenzione dell’analisi - SCADA

In relazione all’ambiente SCADA:

- Gestione delle utenze per le componenti applicative/infrastrutturali
- Privilegi di amministratore in ambiente di produzione, anche di utenze «tecniche»
- Credenziali in chiaro
- Sicurezza della autenticazione delle connessioni tra dispositivi (RTU)
- Struttura documentale sulla sicurezza
- Coinvolgimento della funzione ICT in caso di modifiche manutentive/evolutive
- Governance dei fornitori

Conclusioni

Conclusioni – Aspetti rilevanti nel contesto ICS/SCADA

- Cyber Security a livello board
- Nuove minacce e nuovi attori di attacco
- ICS/SCADA incrementano la superficie di attacco
- Pressione regolatoria in evoluzione: Direttiva NIS sulle infrastrutture critiche
- Skill shortage, soprattutto in ambito ICS/SCADA
- Maturità delle Security Operation, Security Monitoring 24x7x365
- Supply Chain Security

Grazie

Leonardo Nobile
leonardo.nobile@dxc.com

About DXC Technology
DXC Technology (DXC: NYSE) is the world's leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients across 70 countries. The company's technology independence, global talent and extensive partner network combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.com.