COLLOQUIA
INTERNET OF THINGS
NEL CONTESTO DELLE INFRASTRUTTURE CRITICHE

Roma, 26 ottobre 2020 ore 15.00

webinar

programma

14.50	Apertura della sessione e registrazione dei partecipanti
15.00	Apertura dei lavori e saluto **Silvano Bari** (Vicepresidente AIIC) **Glauco Bertocchi** (Vicepresidente IsacaRoma) **Stefano Panzieri** (Università Roma Tre) Presentazione Master "La cybersecurity per la protezione dei sistemi di controllo nell'industria 4.0 e nelle infrastrutture critiche" (industrialsecurity.it)
15.15	**Sandro Bologna** (AIIC) Presentazione Rapporto AIIC **"Internet of Things (IoT) in the context of Critical Infrastructures"** *Il Rapporto è visionabile e scaricabile al seguente link* https://www.infrastrutturecritiche.it/wp-content/uploads/2020/09/GdL-Internet-of-Things_rev-2020.08.12-2.pdf interventi di: **Architettura di un Sistema IoT –** Sandro Bologna **Sicurezza dei Sistemi IoT –** Glauco Bertocchi, Alberto Traballesi **Protezione Dati Personali nei Sistemi IoT** – Luigi Carrozzi **Scenari di Attacco ai Sistemi IoT –** A. Socal, F. Ressa, L. Franchina **Applicazione dei Sistemi IoT nel Mondo Ospedaliero –** Silvano Bari
16.15	*Breve pausa caffè*
16.20	**Emanuele Ermini – Gabriele Mancuso (Siemens)** *IoT: l'approccio Siemens alla sicurezza*
16.40	*considerazioni finali e saluti* **Luisa Franchina (Presidente AIIC)**
16.50	*Chiusura del webinar*

Abstract delle relazioni

Stefano Panzieri (Università Roma Tre)

Professore Associato di Automatica presso Roma TRE. Vicepresidente del Comitato Unico di Garanzia dell'Ateneo Roma TRE. Responsabile del Laboratorio di Modellistica e Simulazione nel settore della Protezione delle Infrastrutture Critiche (MCIP Lab). Coordinatore di Ateneo del progetto per la Regione Lazio Smart Environments. Responsabile di ricerche sul tema della diagnostica energetica nell'ambito Smart Buildings. Coordinatore di alcuni progetti Europei sulle Infrastrutture Critiche. Coordinatore del Dottorato di Ricerca in Ingegneria Informatica e dell'Automazione. Dottore di Ricerca in Ingegneria dei Sistemi nel 1993 alla Sapienza.

Sandro Bologna (AIIC) - Coordinatore GdL "Internet of Things (IoT) in the context of Critical Infrastructures"

Laureato in fisica alla Sapienza, Università di Roma, è membro del Consiglio Direttivo dell'AIIC. Tra le principali attività di ricerca attuali si citano la valutazione della sicurezza, protezione e resilienza di infrastrutture critiche, con particolare riferimento agli aspetti di analisi delle vulnerabilità alle minacce di origine naturale e umana e alla modellistica dei diversi fattori che concorrono a costituire una infrastruttura.

Silvano Bari

Laureato in Scienze Statistiche e Master in Diritto dell'Informatica, già Responsabile Sicurezza e Privacy di Alitalia – Linee Aeree Italiane, attualmente è Professore a contratto di Valutazione del Rischio presso l'Università Campus Bio-medico di Roma e Vicepresidente di AIIC. Certificato CISM.

Glauco Bertocchi

Laureato in Fisica presso l'Università di Roma Sapienza. Più di 40 anni di esperienza in Informatica e Sicurezza nelle Università e nelle Istituzioni Nazionali. Certificato CISM and 27001 LA. Attuali attività di ricerca nel campo della Protezione delle Infrastrutture Critiche e della Resilienza.

Luigi Carrozzi

(CGEIT, CRISC, Auditor L.A. ISMS, ISMS Senior Manager, Privacy Officer) più di 30 anni di esperienza di ICT management in Governance, Risk management e Compliance per primarie organizzazioni private e pubbliche.

Luisa Franchina

E' stata Direttore Generale del Segretariato per le Infrastrutture Critiche (Presidenza del Consiglio dei Ministri 2010-2013). Ha pubblicato un gran numero di articoli e libri sulla protezione e sulla sicurezza delle infrastrutture critiche.

Francesco Ressa

Laureato in Scienze Politiche presso la LUISS Guido Carli e Master in Information Security and Strategic Information presso la Sapienza Università di Roma. Lavora attualmente come analista e consulente presso Hermes Bay SrL sui temi di Enterprise Risk Management, Cybersecurity e Cyber Governance.

Angelo Socal

Senior consultant e security analyst presso Hermes Bay, attivo nei campi di Enterprise Risk Management, Business Economic Intelligence e Cybersecurity. Ha insegnato cybersecurity, risk management, OSINT and SOCMINT presso SIOI, Link Campus University, Sapienza Università di Roma e altri.

Alberto Traballesi

In servizio presso l'Aeronautica Militare Italiana dal 1958 al 1995, congedato con il grado di Generale di Brigata Aereal. Fino al 2013 ha servitor come esparto presso la Presidenza del Consiglio dei Ministri. Laureato in Matematica, Ingegneria Elettronica e Scienze Aeronautiche, attualmente è coinvolto in ricerche sulla protezione ICs e su questioni di politica spaziale.

L'Internet of Things (IoT) è una realtà multiforme: lo troviamo nella domotica, nei sistemi di controllo industriale, nella sanità, nelle automobili e in molti altri contesti. Tuttavia, tutte queste aree condividono alcune funzionalità, spesso inclusi componenti e metodi di accesso alla rete. Proprio queste caratteristiche comuni definiscono anche alcune caratteristiche di sicurezza specifiche. Lo scopo di questo documento è quello di affrontare le caratteristiche specifiche comuni all'IoT e di fornire informazioni sui requisiti di sicurezza dell'IoT, mappando gli asset critici e le minacce pertinenti, valutando i possibili attacchi e identificando potenziali buone pratiche e misure di sicurezza da applicare al fine di proteggere Sistemi IoT, con particolare enfasi nell'ambito delle Infrastrutture Critiche (CI), oltre le "griglie" ai più convenzionali "sistemi vitali", (Servizi Essenziali). Il Rapporto fornisce anche una serie di raccomandazioni per modellare gli sforzi e le iniziative future nella direzione di un approccio olistico per proteggere l'Internet degli oggetti.

A chi è rivolto

Il Documento è rivolto a quei Security Manager e / o Privacy Manager responsabili della compliance in materia di sicurezza e privacy a seguito dell'adozione di sistemi IoT nell'Infrastruttura di cui la Società è responsabile, sia nell'ambito di progetti di innovazione che più semplicemente in evoluzione dei servizi e dei processi esistenti.

Domande chiave affrontate dal documento:

Quali sono le peculiarità della sicurezza IoT?

Quali sono i componenti principali che compongono un IoT?

Quali sono le principali vulnerabilità?

Quali strategie può adottare un'Azienda per mitigarli?

Quali sono i principali problemi di privacy?

Come viene affrontato il problema a livello di standard?

Emanuele Ermini (Esperto Siemens di cyber security) – Gabriele Mancuso (Esperto Siemens HMI) - IoT – L'approccio Siemens alla sicurezza

La sicurezza cibernetica di apparati IOT è l'argomento che ogni settore deve affrontare, dalle infrastrutture all'industria. Siemens con un'architettura di difesa trasversale, ben articolata basata sulla IEC62443, garantisce la sicurezza del dato dalla produzione fino al cloud