ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter
Capitolo di Roma

# Newsletter

ANNO 2019 | N. 02 | NOVEMBRE 2019

## ISACA (Information Systems Audit and Control Association)

L'ISACA, (Information Systems Audit and Control Association), ha più di 145.000 associati in oltre 188 nazioni (dato aggiornato al 2019) ed è l'organizzazione leader nella IT Governance, Security, Controllo ed Assurance. Fondata nel 1969, ISACA promuove conferenze internazionali, pubblica riviste di aggiornamento, sviluppa stardard di Audit & Controllo e amministra le certificazioni professionali CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), CGEIT (Certified in the Governance of Enterprise IT) e CRISC (Certified in Risk and Information Systems Control). I professionisti certificati CISA (dal 1978) sono più di 99500, mentre i CISM (dal 2002) risultano a quota 21000. Le certificazioni CGEIT (introdotta nel 2007) e CRISC (introdotta nel 2010) sono rispettivamente a quota 5400 e 16000.

## EDITORIALE

## Sicurezza logica, fisica e la resilienza. Spunti di riflessione

Obbiettivo di queste brevi note è offrire spunti di riflessione partendo da una sintetica panoramica della sicurezza logica e di quella fisica, della loro "convergenza" e del contributo alla resilienza.

La sicurezza logica, ossia la sicurezza dei dati e delle informazioni in ambito ICT o più correntemente anche se non precisamente cybersecurity, è sicuramente uno degli argomenti più "cool" del momento, se ne parla in tutti gli ambiti, da quello istituzionale a quello professionale nonché nei mezzi di comunicazione tradizionali (radio, tv) e ancor più in Rete.

Esiste ed è sicuramente importante l'esigenza di elevare il livello di sicurezza dei sistemi informatici pubblici e privati e aumentare (spesso partendo da zero) la consapevolezza dei rischi degli utenti della Rete a tutti i livelli. Non mancano le iniziative a livello internazionale e nazionale, ad esempio la direttiva NIS e il regolamento UE 881/2019 (regolamento sulla cybersicurezza), tanto più il recente D.L. 105/2019: perimetro di sicurezza cibernetica, volte a fornire il quadro di riferimento e le relative norme affinché gli stati membri della UE possano iniziare ad operare concretamente in modo coordinato e adeguato al livello della minaccia.

Nel settore privato la rilevanza della materia è evidenziata dal notevole incremento della richiesta di specialisti e dal conseguente svilupparsi delle iniziative di formazione in tema di sicurezza ICT. Si deve però notare che la formazione sembra decisamente in ritardo rispetto alle richieste attuali e a quelle dei prossimi anni (https://www.ispionline.it/sites/default/files/pubblicazioni/ispi_dossier.cyber_.formazione_rugge_dominioni_07.02.2019.pdf).

Le notizie di incidenti ed attacchi cyber però non riguardano solamente i dati bancari o le credenziali degli utenti ma interessano sempre più spesso stabilimenti industriali, mezzi di trasporto, reti di distribuzione di energia, ecc. Un esempio per tutti: l'attacco alla rete elettrica dell'Ucraina con conseguente impossibilità di manovra da parte degli operatori e relativo prolungato blackout.

In sintesi, da diversi anni è crollata la separazione del mondo ICT con quello dell'automazione industriale (o ambito Operational Technology OT) e gli impianti di qualsiasi tipo sono sempre più controllati e gestiti da sistemi ICT spesso non particolarmente sofisticati o aggiornati come, ad esempio, Windows XP che è ancora usato per controllare moltissimi ambiti industriali.

Questa convergenza, o meglio "commistione", è destinata ad aumentare nel futuro, pur con i tempi "prolungati" degli ambiti operativi industriali, a causa dei costi "infinitamente" minori dei sistemi ICT rispetto a quelli dei precedenti apparati "custom" per uso industriale. A tutto ciò si aggiungono i vantaggi derivanti dalla possibilità di interconnessione globale che consente l'uso di Internet.

L'ultimo tassello di questo scenario di cybersecurity è rappresentato dall'irrompere degli IOT (Internet delle cose) con il proliferare di "oggetti" più o

meno "intelligenti" che si possono connettere a Internet e svolgono i compiti più disparati. Il loro numero sarà dell'ordine delle decine di miliardi e l'evoluzione delle telecomunicazioni, come ad esempio il prossimo 5G, ne faciliterà l'utilizzo e quindi lo sviluppo.

In sintesi, la cybersecurity è divenuta pervasiva a causa della progressiva applicazione della Information Technology ad ambiti prima "isolati" oppure inesistenti, come gli IOT. Conseguentemente un incidente informatico può divenire un problema di sicurezza fisica (Safety o Security) perché può alterare il corretto funzionamento di un impianto o un aereo e quindi causare danni alle persone e alle cose.

Cosa era la sicurezza fisica fino a poco tempo fa? Forse si può sintetizzare come protezione dell'incolumità delle persone e tutela dei beni materiali. Come detto prima, la cybersecurity può divenire un aspetto della sicurezza fisica quando un computer controlla operazioni che possono impattare sulla salute o l'incolumità delle persone. Anche qualora la sicurezza fisica si intenda come protezione dei beni, essa è oramai basata sempre più su sistemi di video sorveglianza ed allarme digitali dotati di sensori con indirizzo IP. Il noto caso del malware MIRAI, che consente l'utilizzo fraudolento di telecamere per creare una botnet e sferrare attacchi DDOS, è un esempio dello stato di convergenza tra sicurezza fisica e logica.

Da tempo si parla della necessità di considerare la sicurezza un problema complessivo, ossia a 360°, e superare quindi i "silos" tecnologici, organizzativi e formativi ancora esistenti che impediscono soluzioni integrate e maggiormente efficaci. Sembra arrivato il momento per passare dalla teoria alla pratica e cambiare atteggiamento, a partire da noi professionisti del settore.

L'ultima considerazione riguarda la resilienza che ha nella sicurezza, considerata in tutti i suoi aspetti, una delle componenti fondamentali. Il prevedibile futuro vedrà un sempre maggiore focus sulla resilienza dei sistemi, delle organizzazioni, dei paesi, ecc. È prevedibile un altro cambiamento di paradigma poiché la sicurezza sarà parte di un processo più complesso e si dovranno quindi superare ulteriori "barriere" per integrarla con le altre componenti che contribuiscono alla resilienza (prevenzione, reazione, soccorso, ripristino).

Buona parte di questa evoluzione sarà supportata da strumenti tecnologici, ma la maggior parte di essa comporta cambiamenti di paradigma con conseguenti impatti sulle attività lavorative, sulla governance delle organizzazioni pubbliche e private, sulle scelte formative, ecc. Sarà probabilmente questa la parte più difficile, quella che implica un diverso modo di affrontare i problemi da parte delle persone.

Siamo preparati a questi cambi di paradigma e quanto tempo ci vorrà? Saremo in grado di avere un accettabile grado di resilienza delle attività umane (includendo in esse anche l'utilizzo della robotica e della IA) in un mondo sempre più connesso, complesso e interdipendente?

Glauco Bertocchi
Vice Presidente ISACA Rome Chapter

## NOVITA' DAL CAPITOLO

ISACA Roma è lieta di annunciare l'attivazione del percorso, teorico e pratico con esercitazioni, per ottenere la certificazione "CSX Practitioner Certificate". Il capitolo di Roma è uno dei pochi in Europa e nel mondo ad aver completato l'iter che consente di erogare lezioni anche on-line e di fornire agli studenti la possibilità di esercitarsi con 70 laboratori virtuali.
CSX-P è stato introdotto da ISACA nel 2015 certificazione indipendente dai fornitori e basata sulle abilità a risolvere problemi, per i professionisti dell'information security e cybersecurity. CSX-P richiede ai candidati di dimostrare le proprie capacità nella cybersecurity in un ambiente dinamico e virtuale, cimentandosi su scenari attuali di cyber security, e non semplicemente superare un esame con domande a risposta multipla.
È la sola certificazione completa basata sulle performance individuali nel settore che verifica l'abilità del candidato di svolgere compiti tecnici nelle 5 funzioni di sicurezza definite dal framework NIST – identify, protect, detect, respond and recover. Ai candidati è richiesto di mettere in pratica le competenze acquisite sulla cybersecurity e dimostrare di possedere le abilità necessarie per reagire a un ambiente di minacce cyber sempre più aggressivo e vario.
CSX Practitioner Certificate consiste nel:
1. risolvere i compiti presenti in 10 laboratori virtuali
2. superare l'esame
3. dimostrare di possedere i requisiti per la certificazione (esperienza pluriennale, possesso di ulteriori certificazioni)

Sono disponibili due tipologie di laboratori virtuali:

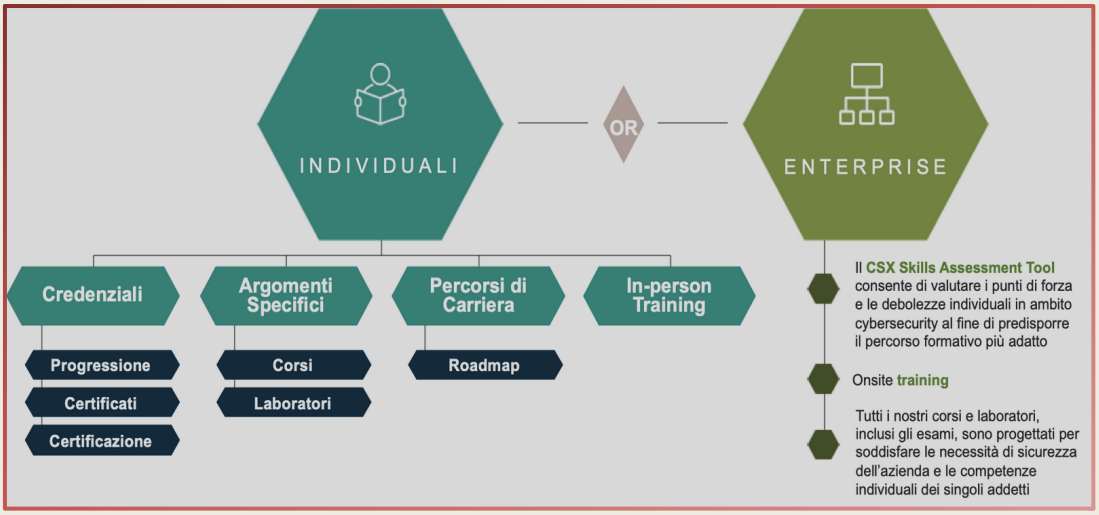
- **Laboratori on-line** – Laboratori realizzati da ISACA International e fruibili come parte integrante dei nostri corsi.
- **Laboratori specialistici esclusivi** – In aggiunta a quelli offerti da ISACA il nostro team di specialisti in ambito cybersecurity e sistemistico ha sviluppato una serie di laboratori indipendenti e utilizzabili off-line.

È stato anche realizzato un laboratorio permanente per sessioni di Cyber Range. L'attività comprende simulazioni di rete ed esercizi di attacchi che permettono ai professionisti della sicurezza di potenziare competenze, esperienza, efficacia, comunicazione e processi

Il partecipante svilupperà competenze pratiche sulla cybersecurity oltre a una solida base teorica, il 50% di tutti i corsi comprende degli esercizi pratici di laboratorio in un **cyber ambiente virtuale**. Nello stesso tempo si approfondiranno le tecniche per rispondere agli attacchi e recuperare dati e sistemi in caso di disastro, in particolare:

- Network evaluation
- Vulnerability analysis
- Malware & incident detection
- Incidence reporting
- Safeguard implementation

L'offerta di corsi CSX è molto varia e modulare, ciò consente anche un approccio graduale e focalizzato su specifici ambiti (penetration e vulnerability, analisys, specialist) per consentire una formazione finalizzata qualora necessaria.




Maggiori dettagli sono disponibili qui:
http://www.isacaroma.it/wp-content/uploads/2019/11/CILLI-CSX_Training_Options_IT.pdf

**ISACA Roma**

- **Segreteria Corsi**
- **Tel. +39 375 599 1500**
- **cybersecurity@isacaroma.it**

**www.csxp.it**

## EVENTI PASSATI

**29 Ottobre 2019** — ***"Gestione del rischio in sistemi interdipendenti: la problematica cyber-fisica"***

- Importanti novità sulla certificazione CSX (Prof. Claudio Cilli – President of the ISACA Rome Chapter);
- Valutazione del rischio in sistemi interdipendenti industriali (Prof. Stefano Panzieri - Professore aggiunto Università di Roma Tre)
- Il problema della cybersecurity nei sistemi di controllo, l'approccio strutturato degli standard (Ing. Chiara Foglietta - Ricercatore presso Università di Roma Tre);
- Event management come contributo alla cybersecurity in ambito industriale (Ing. Riccardo Colelli – Ricercatore presso Università di Roma Tre).

## PROSSIMI EVENTI

### 20 novembre 2019 COBIT 2019 – LA GOVERNANCE SU MISURA

È appena uscita la nuova edizione del framework COBIT, leader tra gli strumenti per la Governance strategica dell'azienda, delle informazioni e della tecnologia (EGIT).

La nuova versione, denominata COBIT 2019, succede al COBIT 5 (del 2012), e, pur garantendo la completa compatibilità con gli investimenti pregressi, contiene, soprattutto da un punto di vista pratico, importanti e significative novità alle quali è dedicato l'incontro odierno.

L'intervento è rivolto sia a coloro che già conoscono il framework COBIT che a chi non ha ancora avuto occasione di approfondirne i contenuti.

Docente: Ing. Alberto Piamonte - Istruttore, Implementor ed Assessor COBIT5

## LE PRINCIPALI NOTIZIE

### CYBER SECURITY, PROFUMO: "CON SAIPEM LAVORIAMO SU PARTE STRATEGICA"

11 Novembre 2019 – "La cooperazione con Leonardo è stata attivata dal momento in cui c'è stato un evento di attacco per Saipem. Abbiamo avuto una prima fase tattica nella quale li abbiamo aiutati a identificare cosa era successo, come isolare la parte sotto attacco, e adesso stiamo lavorando su una parte più strategica volta a costruire un sistema sempre più resiliente a questo tipo di fenomeni".
*(source:https://www.ilmessaggero.it/economia/news/cyber_security_profumo_con_saipem_lavoriamo_su_parte_strategica-4856008.html)*

### CYBER SECURITY, STUDIO CHUBB: AUMENTANO GLI ATTACCHI RANSOMWARE

10 novembre 2019 – Nel corso del terzo trimestre del 2019 gli attacchi ransomware hanno interessato il settore manifatturiero (23%) e quello dei servizi professionali (30%). A sostenerlo è l'ultimo rapporto *InFocus* di Chubb "Adattarsi alle nuove realtà dei cyber rischi".
*(source: https://insurzine.com/cyber-security-studio-chubb-aumentano-gli-attacchi-ransomware/)*

### CYBERSECURITY A PROVA DI 5G, COSÌ NASCE LA "RESILIENCE BY DESIGN"

25 ottobre 2019 – Si alza la sfida sicurezza con il nuovo standard mobile. Ma ai meccanismi già in campo stanno sostituendosi misure di protezione dinamiche. Ecco come Intelligenza artificiale, isolamento delle slice e cognitive radio saranno in grado di rispondere alla nuova generazione di attacchi "zero day"
*(source: https://www.agendadigitale.eu/infrastrutture/cybersecurity-a-prova-di-5g-cosi-nasce-la-resilience-by-design/)*

### ITALIAN POLICE SHUT DOWN DARKWEB BERLUSCONI MARKET AND ARRESTED ADMINS

8 novembre 2019 – Italian law enforcement shut down the 'Berlusconi market' black market and arrested three suspected of being its administrators. Italian financial police "Guardia di Finanza" shut down the 'Berlusconi market' black market hosted on the Tor network...
*(source: https://securityaffairs.co/wordpress/93603/cyber-crime/berlusconi-market-darkweb.html)*

### CYBERSECURITY: COME CAMBIA L'ARCHITETTURA NAZIONALE

8 novembre 2019 – In applicazione di quanto previsto dalla Direttiva Nis – il provvedimento che ha affrontato per la prima

volta a livello europeo il tema della cybersecurity, definendo le misure necessarie a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi – è stato pubblicato in Gazzetta Ufficiale il decreto del Presidente del Consiglio dei Ministri recante disposizioni sull'organizzazione e il funzionamento del Computer Security Incident Response Team – CSIRT italiano.
*(source: http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cybersecurity-come-cambia-larchitettura-nazionale.html*

## CORSI ISACA

### CORSI CISA, CISM, CGEIT E CRISC!

**E' STATO PUBBLICATO IL CALENDARIO DEI PROSSIMI CORSI DI CERTIFICAZIONE ISACA**

Il Capitolo di Roma di ISACA informa che sono aperte le iscrizioni ai corsi di preparazione agli esami di certificazione CISA, CISM, CGEIT e CRISC.
I corsi si terranno a Roma. La sede sarà comunicata prima della data di inizio.
Tutte le informazioni per la registrazione agli esami al seguente link:
http://www.isaca.org/CERTIFICATION/Pages/default.aspx

***DATE***

Corso di preparazione all'esame CISA: **4-5-6-7-8 novembre 2019** e **2-3-4-5-6 dicembre 2019**
Corso di preparazione all'esame CRISC: **1-2-3-4 luglio 2019 e 11-12-13-14 novembre 2019**
Corso di preparazione all'esame CGEIT: **9-10-11-12 dicembre 2019**
Corso di preparazione all'esame CISM: **15-16-17-18 ottobre 2019 e 25-26-27-28 novembre 2019**
Per ulteriori informazioni sui corsi inviare una mail all'indirizzo: **corsi<at>isacaroma<dot>it**


**Cybersecurity Nexus (CSX)** è il programma professionale di ISACA Intl con il quale verranno sviluppate le conoscenze per una corretta gestione della sicurezza informatica. Il programma CSX è il risultato dell'esperienza ultra decennale maturata da ISACA Intl nelle attività di auditing, di gestione dei rischi, del security management e del'IT governance. CSX sta aiutando a plasmare il futuro della sicurezza informatica.

Info e Contatti

info@isacaroma.it

Via Berna, 25 - 00144 Roma

http://www.isacaroma.it/

Social Media

SAPIENZA UNIVERSITÀ DI ROMA