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

Newsletter

ANNO 2020 **N. 01** **GENNAIO 2020**

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 standard 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

Predictions 2020 sulla minaccia informatica per mantenersi pronti.

Gli **aggiornamenti sulla minaccia informatica sono necessari per ogni professionista ICT e di Cybersecurity**, in possesso di una o più delle certificazioni ISACA per prepararsi al meglio lungo il 2020.

Trend tecnologici

La prima necessità è l'individuazione dei principali trend tecnologici perché è proprio su questi che gravano i rischi e si potrebbero concentrare gli attacchi. Secondo Gartner le tecnologie e **infrastrutture 5G** nel 2020 dovrebbe essere implementate dai due terzi delle aziende facendo del 5G, una nuova frontiera appetibile per la minaccia. Subito a seguire la **strategia, applicazione e protezione della convergenza di IT-OT** (Information Technology e Operational Technology), trend iniziato nel 2019 e previsto in espansione nel 2020, che richiederà anche coesione dei team coinvolti, e competenze crescenti dei CISO. Il **massivo ricorso al cloud** nel 2019 da parte di molte organizzazioni ha già innescato problemi crescenti per la sicurezza informatica, per errori di configurazione nei dispositivi di rete e server di applicazioni aziendali portando a dati critici esposti in rete. Il trend **nel 2020 potrebbe crescere in funzione dei "journey to cloud"** intrapresi principalmente dalle istituzioni finanziarie. In aggiunta, il futuro digitale delle imprese nel 2020 (fonte Equinix) prevede: **trasformazione digitale sviluppata in ottica di sostenibilità ambientale, accelerazione del multicloud ibrido in funzione delle esigenze di infrastruttura distribuita ed edge computing, ricorso ad AI e IoT con la conseguente esigenza di elaborazione dei dati** gradualmente crescente in complessità e in tempo reale, per grandi set di dati provenienti da diverse fonti (**interconnessione globale**), **priorità e, infine, le strategie IT per il business aziendale influenzate da regolamentazioni e normative sulla protezione dei dati**.

Cybersecurity predictions 2020

Le previsioni di alcuni dei maggiori vendor di security divulgate recentemente, stimano e descrivono i rischi riguardanti la cyber-security globale per il 2020. Se ne riportano alcuni fra i maggiori che hanno analizzato il panorama della minaccia:

- Secondo Check Point il 2020 sarà caratterizzato da una **nuova guerra fredda cibernetica**, in cui le **fake news influenzeranno** anche le elezioni USA 2020 e gli **attacchi informatici verranno orientati ai servizi pubblici essenziali e infrastrutture strategiche**. Gli attacchi saranno caratterizzati da **ransomware in aumento, Phishing sempre più strutturati, anche via SMS, Malware verso dispositivi mobili e mobile banking**.
- Anche Veritas sottolinea il **pericolo crescente dei ransomware** contraddistinto da una loro evoluzione nelle tecniche di infiltrazione negli ambienti IT per sequestrare dati e tenere in ostaggio organizzazioni del **settore pubblico, dell'healthcare e dell'industria manifatturiera.** Sono questi infatti, gli ambienti **dove i cyber criminali possono colpire grandi volumi di dati e ottenere il massimo ritorno sull'investimento**. In questi settori la strategia di

sicurezza è tradizionalmente debole, ma soprattutto trattano informazioni *mission-critical* nelle loro operazioni quotidiane. Se gli attacchi mirano e riescono ad interrompere i servizi essenziali, le organizzazioni avranno meno tempo per prendere una decisione e saranno più disposte a pagare il riscatto. Lo stesso vale quando **gli attacchi ransomware** sono **focalizzati sulla proprietà intellettuale per esfiltrare dati di prototipi, schemi e progetti dei prodotti e rivenderli ai concorrenti sul mercato nero.** I metodi di **attacco** di **social engineering possono evolvere fino a raggiungere l'intera supply chain** per **ingannare dipendenti, fornitori, liberi professionisti, partner** e far loro condividere verso gli attaccanti informazioni sulle credenziali necessarie ad ottenere le risorse digitali più importanti di un'azienda.

Come **prevenzione** è necessario **migliorare la visibilità su tutti gli asset di dati** e **sfruttare l'automazione** per garantire che i dati siano sottoposti **regolarmente a solide strategie e procedure di backup** per essere recuperabili in ogni momento e luogo. Per **proteggere la supply chain** ogni azienda deve essere certa che ogni potenziale fornitore abbia misure e politiche di protezione dei dati comparabili con le proprie. Fondamentale anche **l'approccio preventivo della formazione** sulla protezione dei dati per i dipendenti a tutti i livelli dell'azienda, e della rete di supply chain. **Periodicamente** sarebbe opportuno **testare le proprie difese** da ransomware ed altri attacchi di social engineering per addestrare il personale in condizioni di emergenza.

- Infine, Darktrace sottolinea i rischi di "cyberwar" e Cybercrime. Nel primo caso anche nel 2020, i danni collaterali provocati dagli attacchi State Sponsored potrebbero causare una guerra informatica con conseguenze nel mondo fisico: ad esempio se un'arma cyber progettata per arrestare un attacco potente e complesso da parte di una nazione, fosse usata invece in modo malevolo per offendere un'altra nazione. Sul fronte del Cybercrime, invece, la conferma dell'**AI come principale tendenza della hacker-sfera.** La "Offensive AI", ovvero la AI usata per attaccare, può produrre **malware sofisticati capaci di adattare** il loro comportamento per non essere rilevati, per ottenere una scalabilità, velocità e automazione, ma anche per comprendere l'ambiente e sfruttare le informazioni ottenute indirizzando meglio l'attacco e contemporaneamente identificando i dati più preziosi da rubare. La AI potrebbe sfruttare la tecnica dell'"Impersonation", che utilizza false identità per ingannare la propria vittima, generando automaticamente e-mail di *spear-phishing*, abili ed efficaci nell'imitare lo stile di scrittura dei contatti personali e dei colleghi più fidati, o per creare video "deepfake" a scopo manipolatorio. Per fortuna la **AI usata anche per la difesa** potrebbe altrettanto rapidamente indagare sulle potenziali minacce, effettuare detection, suggerire azioni di mitigazione e remediation e produrre dei report scritti a misura di analista o manager secondo lo stakeholder di interesse.
- Altre minacce in crescita sono frodi a mezzo *scamming*, truffe del CEO e *cryptominer* (malware progettate per sfruttare fraudolentemente le risorse computazionali di CPU e/o GPU del computer infetto per l'estrazione, o mining, di criptovalute).

L'evoluzione delle minacce informatiche riguarda tutte le categorie di professionisti certificati ISACA**, Auditors** (*Certified Information Systems Auditor, CISA*), **Security Manager, Chief Information Security Officer** (*Certified Information Security Manager, CISM*), **Responsabili IT e Chief Information Officers** (*Certified in the Governance of Enterprise IT, CGEIT e certificati COBIT*), **Consulenti sul rischio di sicurezza informatica** *(Certified in the Risk and Information Systems Control, CRISC*), **esperti e tecnici di sicurezza** (*CSX fundamentals & practitioner*). Infatti, dal punto di vista del ruolo e del lavoro quotidiano e per lo sviluppo continuo delle rispettive competenze per ogni certificazione acquisita e da mantenere, **la conoscenza sulla evoluzione della minaccia per il futuro consente di affrontare in modo consapevole e appropriato le rispettive attività**: effettuare verifiche ispettive con il perimetro di sicurezza adeguato (Auditors), curare la gestione della security e dell'IT (CISO e CIO), implementare la corretta valutazione dei rischi (consulenti, manager CISO e CIO), applicare contromisure preventive e saper effettuare contenimento e remediation in caso di incidenti informatici (SOC e CERT analyst, tecnici, consulenti di sicurezza).

Alessia Valentini
Cyber security consultant, CISA

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:

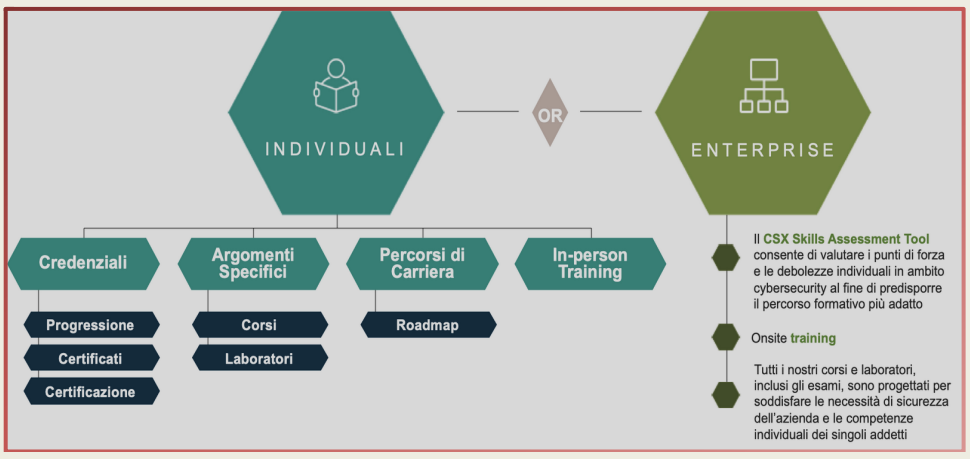
- **Laboratori on-line** – Laboratori realizzati da ISACA International e fruibili come parte integrante dei nostri corsi.
- **Laboratori specialistici esclusivi** – In aggiunta a quelli offerti da ISACA il nostro team di specialisti in ambito cybersecurity e sistemistico ha sviluppato una serie di laboratori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

13 dicembre 2019 UP TO THE CIRROSTRATUS: INCIDENT RESPONSE IN THE CLOUD

Monte dei Paschi di Siena – Sala Azzurra – Via Salaria 231 -Roma - Relatore : Stefano Maccaglia

Stefano Maccaglia ha un'esperienza pluridecennale nel campo della sicurezza informatica. Ha svolto importanti incarichi in Italia e all'estero come consulente specializzato nella investigazione e nella remediation di incidenti. Attualmente opera worldwide per un importante società del settore.
Il Cloud Computing ha cambiato le funzioni e il ruolo dei Data Center tradizionali, introducendo di pari passo, profonde modifiche nelle modalita' di gestione ed esercizio delle infrastrutture IT e la loro messa in Sicurezza.
Proprio su quest'ultimo punto si focalizza il seminario.
Con lo spostarsi in Cloud delle minacce si è notata una maggiore difficoltà nel tracciare e rispondere alle minacce, da un lato a causa dei diversi strumenti che gli analisti devono imparare a padroneggiare, dall'altra perché alcune azioni investigative, consolidate nelle pratiche di Incident Response tradizionali, non sono applicabili in un ambiente Cloud per limiti tecnologici, procedurali o gestionali.
L'intervento presenta una serie di casi reali attraverso cui i partecipanti sono introdotti alle problematiche più comuni e impattanti nella messa in Sicurezza di ambienti Cloud e nella gestione degli incidenti che li coinvolgono.

La documentazione degli eventi passati è disponibile sul sito www.isacaroma.it

PROSSIMI EVENTI

A breve saranno resi noti sul sito e sui futuri numeri della Newsletter le giornate di studio e i seminari del nostro capitolo.

LE PRINCIPALI NOTIZIE

CYBER SECURITY SANITARIA, ECCO LA GUIDA EUROPEA SUGLI STANDARD PER I DISPOSITIVI MEDICI: TUTTI I DETTAGLI

10 gennaio 2020 – La crescente preoccupazione per i rischi posti dalle vulnerabilità nei software medtech ha reso la sicurezza informatica un punto focale per i regolatori di tutto il mondo negli ultimi anni: ora la Commissione UE offre una guida per soddisfare gli standard di sicurezza informatica sui dispositivi medici in Europa.
(source: https://www.cybersecurity360.it/legal/cyber-security-sanitaria-ecco-la-guida-europea-sugli-standard-per-i-dispositivi-medici-tutti-i-dettagli/*)*

COSA SIGNIFICA IL BLITZ CYBER DI ACCENTURE SU SYMANTEC. PARLA ZANERO (POLIMI)

08 gennaio 2020 – La cybersecurity è il mercato del futuro. E con ogni probabilità lo è anche del presente. La protezione di miliardi di dati di altrettante aziende, banche o istituzioni nel mondo è diventata la nuova frontiera. Una certezza per Stefano Zanero, professore associato presso il Dipartimento di Elettronica, Informazione e Bioingegneria del Politecnico di Milano ed esperto di cybersecurity, che a Formiche.net traccia un quadro di un settore letteralmente esploso (nel 2025 il mercato cyber toccherà nel mondo i 205 miliardi di fatturato).
(source: https://formiche.net/2020/01/cibersecurity-italia-iran-zanero-politecnico-usa-guerra-accenture/*)*

PA E DIGITALIZZAZIONE: LA STRATEGIA DEL GOVERNO COMUNICARE MEGLIO CON LE IMPRESE

08 gennaio 2020 – Un nuovo impulso alle attività tese alla digitalizzazione della Pubblica amministrazione arriva dalla legge di Bilancio 2020 e dal decreto Milleproroghe. Viene stabilita, in particolare, l'istituzione di una nuova piattaforma digitale per la notifica di atti, provvedimenti, avvisi e comunicazioni della PA con un risparmio per il bilancio pubblico e minori oneri per i cittadini e le imprese. La piattaforma si legherà all'implementazione dell'identità digitale pubblica o SPID, la cui competenza passa dall'AgID alla Presidenza del Consiglio dei Ministri. Previsti, infine, nuovi stanziamenti di risorse e l'impiego di personale qualificato. Quali saranno gli impatti per le imprese e i professionisti?
(source: https://www.ipsoa.it/documents/impresa/contratti-dimpresa/quotidiano/2020/01/08/pa-digitalizzazione-strategia-governo-comunicare-imprese*)*

SCOPERTE TRE APP ANDROID USATE PER AZIONI DI CYBER SPIONAGGIO: CHE C'È DA SAPERE E COME DIFENDERSI

09 gennaio 2020 – Tre applicazioni regolarmente distribuite su Google Play sono state sfruttate per compiere azioni di cyber spionaggio ai danni di ignare vittime con lo scopo di comprometterne i dispositivi e rubare informazioni riservate. Ecco tutti i dettagli e alcune buone regole di sicurezza per proteggere il proprio dispositivo.
(source: https://www.cybersecurity360.it/nuove-minacce/scoperte-tre-app-android-usate-per-azioni-di-cyber-spionaggio-che-ce-da-sapere-e-come-difendersi/)

TOP 10 CYBERSECURITY PREDICTIONS: 2020 EDITION

08 gennaio 2020 – When I look into my crystal ball at cybersecurity predictions for 2020, I see good news and bad. First, the bad news: Existing threats will worsen, and entirely new threats will arise.
The good news? Job security for cybersecurity professionals will remain for the foreseeable future. Despite the evolution in AI, machine learning and automation technology, humans will continue to be the front line of defense for enterprise cybersecurity. The tools will help, but they cannot replace human intuition and insight.
(source: https://searchsecurity.techtarget.com/tip/Top-10-cybersecurity-predictions-2020-edition)

KASPERSKY: PREVISIONI E TREND PER LA CYBERSECURITY AZIENDALE

09 gennaio 2020 – Per il 2020 Kaspersky ha delineato quali potrebbero essere i rischi e le tendenze della cybersecurity in ambito cloud con attacchi sempre più sofisticati.
Sempre più aziende scelgono di affidarsi al cloud: lo dimostra il numero crescente di realtà professionali che hanno infrastrutture totalmente o parzialmente gestite in questo modo. Questa caratteristica è ormai radicata e il tema della migrazione dei dati verso il cloud è stato uno dei principali trend degli ultimi due anni. Kaspersky ha analizzato la situazione attuale e ha cercato di tracciare uno scenario delle cyberminacce in ambito corporate nel 2020.
(source: https://www.techfromthenet.it/2020010410127/News-analisi/kaspersky-previsioni-e-trend-per-la-cybersecurity-aziendale.html)

NORME CYBERSECURITY IN EUROPA, CHE CAOS: I NODI DA RISOLVERE

03 gennaio 2020 – Con l'ultima raccomandazione della Commissione Ue tornano in primo piano misure basate su policy nazionali. Un ipotetico passo falso nel cammino virtuoso intrapreso finora per ridurre le asimmetrie tra Stati membri. L'analisi dell'iter e gli ostacoli verso un mercato digitale sicuro
(source https://www.agendadigitale.eu/sicurezza/norme-cybersecurity-in-europa-che-caos-i-nodi-da-risolvere/)

L'ITALIA È IL PAESE EUROPEO CHE COMMINA PIÙ MULTE PER VIOLAZIONI DELLA PRIVACY

08 gennaio 2020 – È l'Italia, con 30 provvedimenti del Garante, ad aprire la graduatoria del numero di sanzioni comminate per violazione della privacy. Lo rivela uno studio dell'osservatorio di Federprivacy, la principale associazione di riferimento in Italia dei professionisti della privacy e della protezione dei dati personali, in cui sono state analizzate le attività istituzionali in materia di privacy svolte nei 30 paesi dello Spazio economico europeo (See). Emerge, in generale, che ammontano a circa 410 milioni di euro le sanzioni inflitte nel 2019 per più di 190 procedimenti condotti dalle autorità di controllo per la protezione dei dati personali in Europa.
(source: https://www.wired.it/internet/regole/2020/01/08/privacy-sanzioni-italia-europa/)

CYBER SECURITY, SCOPERTA NUOVA VULNERABILITÀ ZERO-DAY SU MOZILLA FIREFOX

09 gennaio 2020 – Yoroi-Cybaze: scoperta nuova vulnerabilità zero-day su Mozilla Firefox, già usata per attacchi mirati, al fine di installare malware. Installate subito la patch di sicurezza
(source: https://www.difesaesicurezza.com/cyber/cyber-security-scoperta-nuova-vulnerabilita-zero-day-su-mozilla-firefox/*)*

CORSI ISACA

CORSI CISA, CISM, CGEIT E CRISC!

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

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

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.

DATE DEI PROSSIMI CORSI

Corso di preparazione all'esame CISA: **dal 24 al 28 febbraio; dal 23 al 27 marzo 2020;**
Corso di preparazione all'esame CRISC: **dal 4 al 7 febbraio 2020;**
Corso di preparazione all'esame CGEIT: **dal 9 al 12 marzo 2020;**
Corso di preparazione all'esame CISM: **dal 27 al 30 gennaio; dal 17 al 20 febbraio; dal 10 al 13 marzo 2020**
Corso CSX (CyberSecurity Fundamentals): **30-31 gennaio; 27-28 febbraio; 30-31 marzo 2020;**
Corso CSX-P (CyberSecurity Practitioner): **dal 2 al 6 marzo 2020.**
Per ulteriori informazioni sui corsi inviare una mail all'indirizzo: **corsi<at>isacaroma<dot>it**

INFORMAZIONI UTILI

Chi ha già frequentato un corso a pagamento presso ISACA Roma ha uno sconto del 10%.

Aziende, grossi enti, PAL, PAC e Difesa possono richiedere i costi a loro riservati alla casella **corsi<at>isacaroma<dot>it**

Per ulteriori informazioni sui corsi inviare una mail all'indirizzo: **corsi<at>isacaroma<dot>it**

Info e Contatti

info@isacaroma.it
Via Berna, 25 - 00144 Roma
http://www.isacaroma.it/

Social Media

SAPIENZA UNIVERSITÀ DI ROMA