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

Newsletter

ANNO 2020 **N. 05** **MAGGIO 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

Filosofia e applicazioni del MITRE ATT&CK framework

Dice il saggio popolare:" la miglior difesa è l'attacco", mentre Sun Tzu ne "L'arte della guerra" esalta la conoscenza di sé stesso e dell'avversario come chiave della vittoria. Ma cosa conoscere del nemico per prevenirne le mosse e batterlo, o meglio ancora, per renderlo inoffensivo? Se Sun Tzu, definisce il condottiero migliore, come colui che è capace di vincere senza combattere, allora per "vincere a mani basse" (come dicono i pugili) è necessario conoscere le tecniche di attacco dell'avversario e predisporre una difesa congrua. Esattamente con questo fine, è stato creato ed è comunemente utilizzato, il **MITRE ATT&CK Framework**, una base di conoscenza di Tattiche e Tecniche e Procedure (TTPs) degli avversari, tipicamente malevoli, basate su quanto avviene nello scenario Cyber Mondiale. La knowledge base di ATT&CK è usata come base per lo sviluppo di specifici modelli e metodologie di minaccia (Threat Models) nel settore privato, nel governo e nella comunità dei prodotti e servizi per la sicurezza informatica. ATT&CK è rappresentato come una tassonomia comprendente sia l'attacco che la difesa (con le opportune corrispondenze) ed è diventato un utile strumento concettuale per veicolare informazioni sulle minacce, effettuare test o emulare l'avversario al fine di migliorare le difese di rete e di sistema contro le potenziali intrusioni. Il framework permette anche di gestire meglio il rischio informatico e pianificare quali dati devono essere disponibili per il rilevamento della minaccia informatica o per indagare su un incidente di sicurezza. Creato a partire dal 2010 è stato evoluto fino ad oggi e continuerà ad essere integrato con le tecniche, tattiche e procedure di attacco usate correntemente dai criminali digitali, facendo corrispondere le più appropriate tecniche di difesa.

Concettualmente sono tre le idee alla base della filosofia con cui è stato concepito il framework: mantiene la prospettiva dell'avversario, usa esempi empirici sfruttando quello che avviene nel mondo reale e fornisce un livello di astrazione appropriato per contrastare l'azione offensiva con possibili contromisure difensive eventualmente preventive.

L'ATT&CK per le Enterprise è rappresentato da una matrice di corrispondenza fra l'insieme di tecniche e sub-tecniche e le tattiche utilizzabili per raggiungere

e violare un target. Per ognuna delle fasi di attacco è riportata la lista in colonna delle tecniche utilizzabili. Gli step di attacco elencati sono: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact. Per ognuno è fornita la lista delle tecniche utilizzabili, mentre per ogni tattica esiste una scheda di dettaglio con le indicazioni dei gruppi che tipicamente ne fanno uso, la descrizione di esempi e ovviamente delle tecniche di mitigazione e detection più appropriate. Alcune tecniche possono essere suddivise o composte da sotto-tecniche che delineano in modo più dettagliato il comportamento durante l'esecuzione da parte degli attaccanti. Il MITRE Framework si presenta per diversi domini tecnologici. tre sono le maggiori categorie: Enterprise, Mobile e i sistemi di controllo industriale (ICS). Per ciascuna sono elencate le piattaforme o i sistemi applicabili. Così in ambito Mobile vi sono descrizioni sia per i sistemi IOS che per Android, mentre in ambito Enterprise le entità maggiormente attaccabili a cui le TTPs fanno riferimento sono: Linux, macOS, Windows, AWS, Azure, GCP, SaaS, Office 365, Azure AD. Per gli ICS sono analizzati i sistemi SCADA su cui le tecniche sono applicabili.

Le modalità di adozione e uso di ATT&CK sono molteplici. Nella **emulazione dell'avversario** il Framework permette di creare scenari di simulazione per testare e verificare le difese contro le tecniche degli avversari. La profilazione di gruppi specifici di attaccanti (come apt29 ad esempio) può essere costruita sulla base di informazioni di Cyber Threat Intelligence presenti nel Framework, ovvero secondo le TTPs più comunemente usate dal gruppo di attacco d'interesse. Al Profilo dello specifico gruppo di attacco si possono coniugare, allineare e migliorare le misure difensive.

Nel **Red teaming**, in cui si cerca di effettuare un breach in una rete target per mostrarne l'impatto rovinoso, il framework si presta per creare piani di attacco capaci di evitare difese attive all'interno di una rete e per sviluppare nuovi modi di eseguire azioni non rilevabili dalle difese standard. Anche nella **misura di maturità del SOC aziendale**, ATT&CK può consentire la valutazione di efficacia in relazione ai processi e tempi di rilevazione, analisi e risposta alle intrusioni. Similmente, nella determinazione dei **Gap nella difesa** di un perimetro aziendale, ATT&CK abilita la capacità di individuare lacune e punti ciechi per i potenziali vettori di attacco che potrebbero generare un incidente informatico.

Quando ci si occupa di **analisi di tipo comportamentale della minaccia** (behavioural analytics) piuttosto che la ricerca di Indici di compromissione (IOCs) si rilevano attività potenzialmente dannose che costituiscono i comportamenti malevoli; in questo ambito ATT&CK si presta come strumento per costruire e testare analisi comportamentali capaci di rilevare eventi ed evidenze contraddittorie all'interno di un ambiente. Infine, il Framework si presta per il processo di **enrichment della minaccia** ovvero per comprendere e documentare il profiling degli attaccanti in modo indipendente dagli strumenti di attacco usati. Attenzione, l'attribuzione non dipende solo ed esclusivamente dalle tecniche di attacco poiché più gruppi potrebbero fare uso delle stesse tecniche, ma si ricercano similitudini del modus operandi anche grazie al Framework MITRE.

Naturalmente il Framework può essere arricchito da nuove tecniche, tattiche e procedure non appena sono scoperte nel panorama della minaccia. Il tutto avviene in modalità trasparente mediante un processo decisionale altrettanto chiaro ed esplicito, affinché lo strumento possa continuare a beneficiare della fiducia da parte di tutti gli utilizzatori per le informazioni e risorse che lo compongono.

Alessia Valentini
Cyber security consultant, CISA

NOVITA' DAL CAPITOLO

ACCORDO

È stato sottoscritto un accordo tra **ISACA Roma** e l'**Istituto Italiano di Project Management® (ISIPM)**, con il quale le due associazioni intendono promuovere e sviluppare un processo di collaborazione, nelle aree culturali di comune interesse di "Project Management" e ICT Security Management, attraverso l'organizzazione e la realizzazione di attività congiunte, al fine di promuovere i principi e le tecniche professionali.
L'intenzione è quella di:

- avvicinare le community nazionali di **ISIPM** e **ISACA**
- ampliare le aree di interesse delle due community
- favorire lo scambio di esperienze e conoscenze
- aumentare il grado di formazione e di competenza nelle tematiche di interesse delle due organizzazioni
- organizzare congiuntamente eventi e/o webinar di "Project Management" e ICT Security Management, per sensibilizzare i propri soci sull'importanza di tali discipline e delle relative metodologie e tecniche.
- sviluppare percorsi formativi congiunti, che uniscano la formazione per le certificazioni di **ISACA** (**CSX® fundamentals**, **CSX-P**, **CISA®**, **CISM®**, **CGEIT®** e **CRISC®)**, a quella per la certificazione **ISIPM-Base®** e alla qualificazione **ISIPM-Av®** di **ISIPM** (1° e 2° livello di certificazione PM). L'obiettivo è fornire le competenze organizzative, tecniche, ed operative in materia di **Cyber-Security,** insieme alle conoscenze di **Project Management**, utili e necessarie per coloro che partecipano a progetti in vari ruoli o intendono qualificarsi.
- sviluppare e sostenere gruppi di lavoro congiunti, per studiare e creare nuove opportunità, che possono avvicinare sempre di più le due discipline, su obbiettivi comuni.

Seguiteci nei prossimi giorni, così sarete sempre aggiornati e potrete scoprire tutte le attività e le novità in arrivo.

Informiamo i Soci e i followers di ISACAROMA che, a seguito delle disposizioni volte a contrastare la diffusione del virus COVID-19 (Coronavirus), abbiamo dovuto rinviare lo svolgimento dei consueti seminari in presenza.

Abbiamo quindi predisposto lo svolgimento di eventi on-line a partire da Aprile. Le modalità di informazione sono, oltre al sito www.isacaroma.it, le consuete mail di annuncio/invito spedite ai contatti della nostra mailing-list che coincide con la diffusione della Newsletter. Per iscriversi alla mailing list è sufficiente inviare una mail con oggetto SUBSCRIBE a eventi@isacaroma.it

Speriamo, soprattutto per il bene del nostro paese, che questa situazione emergenziale finisca presto. Noi saremo pronti a riprendere gli eventi in presenza appena sarà possibile.

Vi terremo informati, per il momento vi auguriamo buona lettura!

ISACA Roma ha attivato il 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:

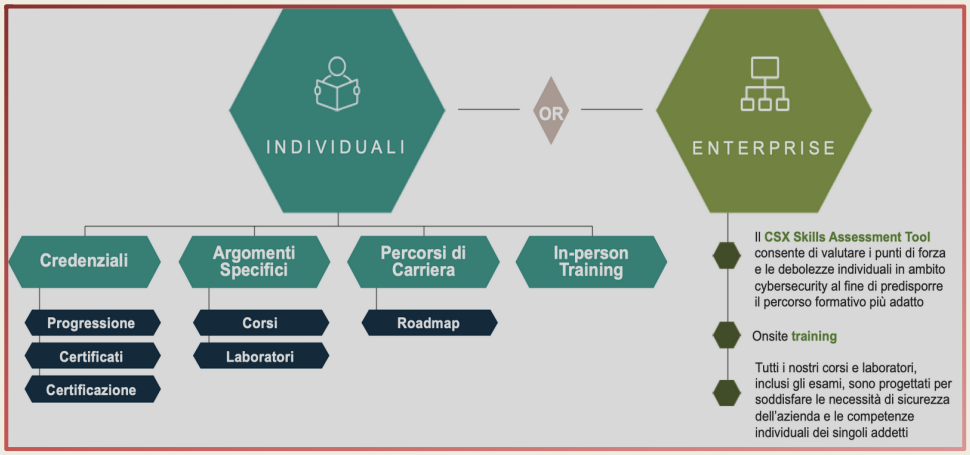
- **Laboratori on-line** – Laboratori realizzati da ISACA International e fruibili come parte integrante dei nostri corsi.
- **Laboratori specialistici esclusivi** – In aggiunta a quelli offerti da ISACA il nostro team di specialisti in ambito cybersecurity e sistemistico ha sviluppato una serie di laboratori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

WEBINAR del 10 aprile 2020

"COSA ACCADE SE DUE DIVERSI ATTACCANTI SOFISTICATI SI CONTENDONO IL DOMINIO DI UNA RETE: LEZIONI APPRESE DA CASI REALI "

Relatori: Stefano Maccaglia e Marco Faggian

Stefano Maccaglia Stefano è Senior Principal Consultant nel team di Incident Response di RSA dal 2012 e ha alle spalle numerose investigazioni su incidenti di grandi dimensioni in varie parti del mondo. Hacker della prima ora, nonché antropologo e sociologo, nel suo percorso lavorativo ha collaborato con molte realtà di primo piano del panorama ICT mondiale, da Digital a Cisco. Speaker abituale di conferenze internazionali, al di fuori del lavoro è attivo nella produzione di contributi sulle tematiche della cybersecurity e del cyber-spionaggio.

Marco Faggian lavora in RSA dal 2012, prima come delivery specialist e poi come consulente di Incident Response. Laureato in Ingegneria Informatica a Padova, inizia la sua carriera lavorativa occupandosi dei temi legati alla cybersecurity, collaborando con diverse realtà di consulenza in Italia ed Inghilterra. La sua attività lo porta a seguire alcuni fra i più importanti clienti dei diversi settori fra cui Bancario/assicurativo, Pubblica Amministrazione e Manufatturiero.

WEBINAR del 30 aprile 2020

"POSEID-ON: IL PROGETTO EUROPEO SULL'IDENTITÀ DIGITALE"

Relatori: Roberta Lotti MEF) - Barbara Intonti (Accenture) - Livia Zampolini (Accenture) - Dario Beltrame (Accenture) - Giovanni Maria Riccio (E-LEX)

Il progetto prevede la realizzazione di una piattaforma sicura di Personal Data Management, compliant al Regolamento GDPR.
INTRODUZIONE AL PROGETTO PoSeID-on: • Obiettivi e challenge • Principali elementi di valore ed innovazione • Elementi di compliance al GDPR• Risultati […].

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

PROSSIMI EVENTI

Con i consueti canali (mail, sito, numeri della Newsletter) vi informeremo delle prossime giornate di studio e dei seminari del nostro capitolo.

*Abbiamo programmato un webinar per **venerdì 15 maggio 2020 dalle ore 15:00, alle ore 17:00** dal titolo **How to define and build threat intelligence capability** tenuto dal prof. Claudio Cilli (Recognised international authority in the areas of National Security and Intelligence, company protection, information systems security and compliance, with over 25 years of experience. Adjunct Professor at Rome University.*

CIA, CISA, CISM, CGEIT, CRISC, CISSP, CSSLP, HCISPP, M.Inst.ISP. President of the ISACA Rome (Italy) Chapter).

Il seminario è riservato alle persone che sono già inserite nella nostra lista di inviti . *Qualora voleste essere inseriti nella suddetta lista per i prossimi eventi è sufficiente inviare una mail con oggetto SUBSCRIBE a eventi@isacaroma.it*

LE PRINCIPALI NOTIZIE

BUSINESS CONTINUITY, CSQA PUBBLICA NUOVA GUIDA E LISTA DI RISCONTRO PER LA VALUTAZIONE

06 maggio 2020 – Disponibile la **NUOVA GUIDA e la LISTA DI RISCONTRO PER LA VALUTAZIONE** della edizione aggiornata della norma **UNI EN ISO 22301:2019 Sicurezza e resilienza - Sistemi di gestione per la continuità operativa (SGCO).**

(source: https://www.csqa.it/Sicurezza-ICT/News/Business-continuity,-CSQA-pubblica-nuova-guida-e-l)

CYBER-SECURITY, ARRIVA IL NUOVO CSIRT (FIRMATO DIS). ECCO COME FUNZIONERÀ

07 maggio 2020 – La sicurezza cibernetica in Italia entra nel vivo. È stato inaugurato mercoledì 6 maggio il Csirt Italia (Computer Security Incident Response Team), il nuovo team per gestire la cyber-difesa nazionale istituito presso il Dis (Dipartimento informazioni per la Sicurezza).
Previsto dalla Direttiva Nis (dl 65/2018), il Csirt sostituisce il Cert-Pa e il Cert nazionale, le due strutture che finora hanno supportato rispettivamente le pubbliche amministrazioni e il settore privato nella prevenzione e nella risposta agli incidenti cyber.

(source: https://formiche.net/2020/05/cyber-security-nuovo-csirt-dis/)

FATTORE UMANO E ATTACCHI APT: TECNICHE OFFENSIVE E STRATEGIE DI REMEDIATION

08 maggio 2020 – Il fattore umano è un aspetto spesso trascurato nelle strategie di difesa dagli attacchi APT eppure fondamentale per la sicurezza del perimetro aziendale. Non potendo, però, eliminare le naturali e fisiologiche vulnerabilità dell'essere umano, sarebbe quantomeno opportuno limitare la cosiddetta esposizione iniziale. Ecco in che modo.

(source: https://www.cybersecurity360.it/nuove-minacce/fattore-umano-e-at-tacchi-apt-tecniche-offensive-e-strategie-di-remediation/)

COVID-19, SUPERCOMPUTER ITALIANI AL SERVIZIO DELLA LOTTA AL VIRUS

08 maggio 2020 – La ricerca è impegnata su più fronti nell'emergenza Covid-19 a cominciare dall'individuazione di farmaci efficaci e dalla messa a punto di vaccini in grado di scongiurare il ritorno in futuro di una pandemia come quella che stiamo vivendo. In questa corsa contro il tempo la velocità di calcolo dei supercomputer gioca un ruolo determinante nel lavoro dei ricercatori. CINECA, CMCC, ENEA, INFN-CNAF, che rappresentano i principali enti di supercalcolo in Italia, in un'iniziativa promossa dall'Associazione Big Data in stretta cooperazione con la Fondazione internazionale "Big Data and Artificial Intelligence for Human Development", mettono a disposizione dei ricercatori per progetti volti alla lotta e al contenimento dell'epidemia COVID-19A oltre 8 milioni di ore di calcolo a disposizione.

(source: http://www.askanews.it/scienza-e-innovazione/2020/05/08/covid-19-supercomputer-italiani-al-servizio-della-lotta-al-virus-pn_20200508_00055/)

L'INTELLIGENZA ARTIFICIALE AL TEMPO DEL SOCIAL DISTANCING

08 maggio 2020 – L'inizio della "fase due" segnerà la fine del "lockdown" deciso dal governo Conte per contenere l'epidemia di Covid19: gli italiani torneranno progressivamente a frequentare il loro posto di lavoro affollando uffici e aziende che ora richiedono misure di sicurezza nuove, come ad esempio il monitoraggio all'entrata della temperatura di centinaia di migliaia di individui, per individuare tempestivamente nuovi possibili casi.

(source: https://www.ansa.it/osservatorio_intelligenza_artificiale/notizie/societa/2020/04/21/ai-thermometer-e-social-distancing-i-software-delliit-che-misurano-temperatura-e-distanza-grazie-allintelligenza-artificiale_04f38efe-0ecb-4c98-b346-0d5d2b72d24a.html)

INFODEMIA DA CORONAVIRUS. COSÌ L'INTELLIGENZA ARTIFICIALE HA PERMESSO DI STUDIARLA

09 maggio 2020 – Il rischio di troppe informazioni, spesso non accurate, che disorientano è stato segnalato anche dall'Organizzazione mondiale della sanità. Con algoritmi di IA è stato possibile capirne di più.

(source: https://www.corriere.it/salute/ehealth/cards/infodemia-coronavirus-cosi-l-intelligenza-artificiale-ha-permesso-studiarla/deformazione-realta-allerta-oms_principale.shtml)

HOW COVID-19 IS EVOLVING THE DATA BREACH COMMUNICATION PROCESS

07 maggio 2020 – Covid-19 is at the forefront of business minds right now, with many tasking themselves with understanding, reacting to and learning lessons from this ever-changing situation. However, although business survival will be the top priority throughout this pandemic, it's also essential to have the correct processes in place to effectively respond to a data breach.

(source: https://www.finextra.com/blogposting/18738/how-covid-19-is-evolving-the-data-breach-communication-process)

CORSI ISACA

CORSI CISA, CISM, CGEIT E CRISC!

COME IMMAGINATE L'EMERGENZA COVID-19 E LE CONSEGUENTI RESTRIZIONI NORMATIVE HANNO PORTATO AL RINVIO A NUOVA DATA DEI CORSI DI ISACA ROMA. STIAMO VALUTANDO COME SOPPERIRE NEL MIGLIOR MODO POSSIBILE.

CISA CISM CGEIT CRISC

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.

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