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

# Newsletter

ANNO 2022 N. 8 SETTEMBRE

## ISACA (Information Systems Audit and Control Association)

L'ISACA, (Information Systems Audit and Control Association), ha 153.800 associati in oltre 188 nazioni (dato aggiornato al 31 agosto 2021) 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), CRISC (Certified in Risk and Information Systems Control) e CDPSE (Certified Data Protection Solutions Engineer) . 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

## LA DIFESA DEL REVERSING NEGLI ATTACCHI DDOS

Tutto il 2022 è stato caratterizzato da un aumento significativo dell'attività di attacco di tipo DDoS in tutto il mondo. Gli attacchi hanno ricompreso casistiche motivate da attivismo ma anche a seguito del conflitto Russo Ucraino con attacchi terabit in Asia e negli Stati Uniti. (Fonte *2022 H1 Global Threat Analysis Report* di Radware e report "*2022 Q2 DDoS report*" di Cloudflare)

In Italia l'annuncio di innalzamento del rischio di attacchi DDOS è avvenuto a cura del CSIRT a partire da Maggio 2022 mediante uno *specifico annuncio* mirato a fornire una panoramica sugli episodi di DDOS di tipo "Slow HTTP", descriverne la tecnica di funzionamento e suggerire alcune misure di mitigazione applicabili.

L'attacco DDOS, acronimo di Distributed Denial of Service, avviene quando più sistemi informatici compromessi attaccano un obiettivo e causano una "negazione del servizio" per gli utenti della risorsa presa di mira. La destinazione può essere un server, un sito Web o un'altra risorsa di rete. Il flusso di messaggi, come ad esempio richieste di connessione o pacchetti in formato errato in arrivo al sistema di destinazione, lo costringe a rallentare o addirittura a bloccarsi e spegnersi, negando così il servizio ai legittimi utenti o sistemi.

La mitigazione di un DDOS e/o l'intera gamma di azioni preventive dipendono dal tipo di DDOS ovvero dalle tecniche usate dagli attaccanti per effettuarlo.

Fra i diversi tipi di DDOS si distinguono quelli incentrati sulla rete o cosiddetti volumetrici, attacchi di protocollo, attacchi al livello applicativo e gli attacchi DDOS alle reti IoT (Fonte *Techtarget*). Fra le varie modalità e tecniche usate dagli attaccanti per causare un DDOS c'è l'uso dei cosiddetti booter, o "network stress tester", servizi solitamente costituiti da server dedicati compromessi che inviano enormi quantità di traffico. I booter sono relativamente economici ed estremamente facili da usare. Spesso sono utilizzate anche le BOTNET ovvero reti di computer infetti che agiscono come zombie sincronizzati dagli attaccanti per lanciare richieste di connessione ad un target predefinito. Il danno derivante dal downtime è chiaramente legato alla tipologia dell'utenza e al tipo di servizio digitale di cui non si può usufruire, Infatti, per alcuni servizi come l'e-commerce, il cliente si potrebbe rivolgere alla concorrenza causando perdite economiche difficilmente reversibili al soggetto vittima.

Un'efficace soluzione a questi attacchi, chiamata spesso "reversing", è costituita dalla adozione di un "Web reverse proxy" in breve, "reverse proxy" o "proxy inverso", spesso coniugandolo anche alla tecnica di caching.

Un server proxy inverso funge da punto intermedio posizionato al confine di una rete. Agisce come un endpoint, ricevendo tutte le richieste HTTP per la connessione e le invia al server preposto all'interno della rete. Il server proxy agisce come una "guardia nel traffico di rete" e da gateway dal server di origine rispetto agli utenti. Quando il proxy è sufficientemente potente, agisce ed è efficace contro i DDOS poiché si può dire che tutti gli attacchi di rete diretti al server "colpiranno un muro" quando raggiungono il proxy inverso. La sua presenza riduce la superficie di attacco mitigando tutti gli attacchi di rete che non raggiungono mai il server target.

Il Reverse Proxy viene comunemente associato al caching, che riduce ulteriormente la superficie di attacco e, in particolare, blocca anche gli attacchi delle applicazioni.

Normalmente il caching o la memorizzazione nella cache è una tecnologia che permette di memorizzare le pagine Web in un server proxy di tipo standard. In un attacco DDoS, numerose richieste a una singola risorsa risulteranno in una sola richiesta al server e quindi il server non subirà l'impatto dell'attacco.


Quando le tecnologie di Reverse Proxy e di caching son combinate insieme, sono in grado di "bloccare" praticamente tutti gli attacchi di rete, gli attacchi delle applicazioni alle pagine statiche e in parte, altri tipi di attacchi. Questa combinazione di tecnologie è considerata uno dei metodi più efficaci contro gli attacchi DDoS.

Due sono gli accorgimenti principali quando si usa il reversing:

Stando sulla frontiera della rete, anche il reverse proxy può essere soggetto ad un DDOS ed è quindi buona norma impostarne più di uno, in modo che il web server principale del generico servizio "AAA" si trovi dietro più server reverse proxy. In questo modo, se qualcuno sceglie colpire il generico sito "AAA.com" solo uno dei reverse proxy risulterà colpito, ma i client potranno comunque connettersi al servizio tramite gli altri server alternativi.

Il secondo accorgimento riguarda il fatto che i reverse proxy possono costituire un "single point of failure" nell'architettura di rete, per come sono posizionati. Quindi è fondamentale monitorarne il funzionamento continuamente per evitare che un errore all'interno di questi server possa compromettere le prestazioni e la disponibilità dell'intero sistema. I moderni server reverse proxy sono in grado di eseguire il bilanciamento del carico di livello 7 (applicazione) e livello 4 (trasporto) (della pila ISO/OSI n.d.r.) risultando più affidabili. Il livello iniziale dei sistemi di bilanciamento del carico di livello 4 può distribuire il traffico in entrata ai sistemi di bilanciamento del carico proxy, il che consente loro di funzionare su più nodi. I modelli a due livelli sono ideali per il bilanciamento di carico dei sistemi di storage, che sono diventati sempre più popolari negli ultimi anni.

Si ricorda infine, che i reverse proxy hanno anche altri utilizzi e vantaggi oltre all'uso nella sicurezza informatica: sono tipicamente usati per load balancing, per realizzare un caching potenziato, per la compressione del traffico, per la crittografia SSL ottimizzata, per *ottimizzare i test di tipo A/B* e per introdurre l'autenticazione ad un web server che ne è sprovvisto (Fonte *Network management Hub*).

Alessia Valentini
Cyber security consultant, CISA

## NOVITA' DAL CAPITOLO

ISACA Sistemi informativi: averne fiducia e trarne valore Rome Chapter

# ACCORDO

Istituto Italiano di Project Management

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.

**Informiamo i Soci e i followers di ISACAROMA che stiamo proseguendo con lo svolgimento di eventi on-line. Le modalità di informazione sono 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*.**
**Vi terremo informati su eventuali eventi in presenza, per il momento vi auguriamo buona lettura!**

---

## EVENTI PASSATI

***VEN 16 SETTEMBRE 2022 ORE 15:00-17:00***

# "LE ANALISI DEI RISCHI NEL GDPR"

*A differenza della DPIA (art. 35) che deve essere eseguita solo nei casi espressamente previsti dalla normativa o quando si è in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche, le analisi dei rischi previste dagli artt. 24, 25 e 32 del GDPR sono sempre obbligatorie, per lo più disattese, e non riguardano solo aspetti di sicurezza.*

*Vi è quindi una diffusa incoerenza fra quanto richiesto dalla normativa e quando effettivamente agito. Se da un lato questo si traduce in una estesa mancanza di conformità da parte dei Titolari, dall'altro risultano carenti le adeguate misure tecniche ed organizzative poste a tutela delle persone fisiche ed i loro diritti.*

*Anche quando l'analisi dei rischi viene effettuata in molti casi l'approccio è completamente errato, in quanto si valutano le conseguenze per il Titolare e non, come richiesto dalla normativa, quelle sui diritti e libertà delle persone fisiche.*

*Qual è quindi il corretto approccio a questi adempimenti e quali sono gli strumenti che il Titolare ha a disposizione?*

**Il relatore:** ***Giancarlo Butti***
***Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni.***

***Oltre 150 corsi e seminari tenuti presso ISACA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DI MILANO, CEFRIEL, AIIA, ABI…; già docente del percorso professionalizzante ABI – Privacy Expert e Data Protection Officer e di master presso diversi atenei.***
***Ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate.***
***Ha pubblicato 25 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 23 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT. Socio e già proboviro di AIEA è socio del CLUSIT e del BCI. Partecipa a numerosi gruppi di lavoro.***
***Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMBCI.***

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

## PROSSIMI EVENTI

***GIOV 27 OTTOBRE 2022***

***ORE 15:00-18:30***
*(4CPE)*

## *" Utilizzo dei framework (Iso 2700, NIST, ecc) e analisi del rischio quantitativa. Un primo passo dalla conformità all'efficacia."*

*Il webinar ha l'obiettivo di illustrare i risultati ottenuti dal Gruppo di lavoro di ISACA Roma che si è occupato di utilizzo di framework, in particolare* ***dell'ISO 27002: 2022****, per l'analisi del rischio quantitativa.*
*Il lavoro, inizialmente nato con l'obiettivo di definire un bridge tra ISO 27001 e FAIR (webinar 29 gennaio 2021), è evoluto includendo l'analisi delle problematiche presenti nei framework nati per la conformità ed il loro uso per l'analisi quantitativa del rischio (webinar 29 0ttobre 2021).*
***La nuova versione degli standard ISO2700, e in particolare dell'ISO 27002:2022 è stata l'occasione per approfondire alcuni aspetti fondanti dei framework e delle problematiche relative al loro "mapping" con ontologie e metodi di analisi quantitativa del rischio (nel nostro caso il FAIR).***
***Ne è risultato un panorama molto complesso, che getta una nuova luce sull'approccio con cui considerare i framework, la loro applicazione e le problematiche per la loro "interfaccia" con metodi e strumenti quali quelli dell'analisi del rischio. In pratica un primo passo per utilizzare l'ISO 27000 anche per valutare la sua efficacia.***
***I risultati del Gruppo non sono stati limitati allo studio e all'elaborazione "teorica" di metodi di analisi e calcolo ma ogni ipotesi è stata tradotta in modelli che hanno consentito di esplorarne la validità. Ne è nato anche un tool, a fini dimostrativi e sperimentali.***

Hanno partecipato (in ordine alfabetico) ***Glauco Bertocchi; Giuseppe Cagnetta, Francesca Della Mea, Luca Fei, Maurizio Pagano, Alberto Piamonte, Mario Taddonio, Alessia Valentini***

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

***Gli annunci e gli inviti saranno spediti con le consuete modalità agli iscritti alla nostra mailing list.***

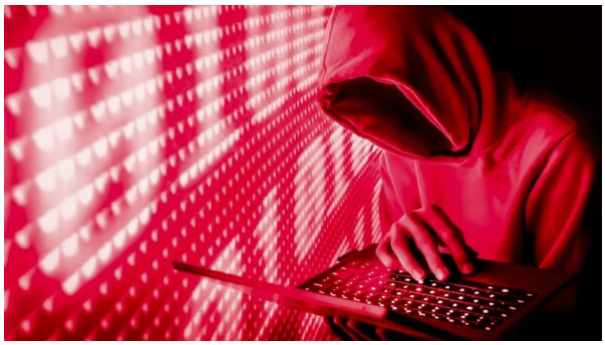
***I non iscritti possono ricevere tali comunicazioni inviando una mail con oggetto "subscribe" contenente solo nome e cognome a eventi<at>isacaroma.it***

## LE PRINCIPALI NOTIZIE

### CYBERSECURITY: COME L'AI PUÒ POTENZIARE LE DIFESE

21 settembre 2022 – Nei primi 6 mesi del 2022 gli attacchi malware su scala globale sono stati 2,8 miliardi mentre Kaspersky ha rilevato in media 380mila file infetti quotidianamente nel 2021. Ecco come grazie alla tecnologia AI la sicurezza informatica può essere rafforzata automatizzando diverse attività demandate agli analisti.
*(source: https://www.ai4business.it/intelligenza-artificiale/ai-cybersicurezza/)*

### COME CAMBIA LA CYBERSECURITY CON IL DL AIUTI BIS? RISPONDE IEZZI (SWASCAN)



19 settembre 2022 – *Le novità sulla reazione agli attacchi sono "cruciali" per il Paese. "Il passo successivo e forse più complesso, sarà sicuramente quello dello stabilire i processi di implementazione", spiega l'esperto di cybersecurity*
"Il decreto-legge Aiuti bis richiama disposizioni cruciali per la cyber sicurezza del nostro Paese", spiega **Pierguido Iezzi**, ceo di Swascan, parte del polo cyber di Tinexta Group, commentando con *Formiche.net* le misure in materia di intelligence in ambito cyber previste.
*(source: https://formiche.net/2022/09/decreto-aiuti-bis-cyber-iezzi-swascan/ )*

### EUROPEI DI CYBERSECURITY 2022: LA NAZIONALE ITALIANA SFIORA IL PODIO

21 settembre 2022 – L'era digitale ha portato numerosi vantaggi alla nostra società, ma ci ha anche reso possibili vittime di nuove tipologie di pericoli, insediati nei più fitti meandri della rete. Grazie all'evoluzione tecnologica, siamo stati in grado di connetterci l'un l'altro anche a migliaia di km di distanza. La digitalizzazione ha contribuito in modo sostanziale alla creazione di un modello di vita nettamente più rapido e più efficiente rispetto agli standard del passato.
*(source: https://www.millionaire.it/europei-di-cybersecurity-2022-la-nazionale-italiana-sfiora-il-podio/)*

### CYBERSECURITY, COSA FARANNO INSIEME LEONARDO ED ENGINEERING

20 settembre 2022 – Leonardo ed Engineering si alleano per accelerare la transizione digitale del Paese.
Il colosso della difesa e aerospazio e il gruppo leader nei processi di trasformazione digitale per aziende e Pa "hanno siglato un MoU (Memorandum of Understanding), iniziando una collaborazione strategica per individuare progetti e opportunità di business da sviluppare congiuntamente nel campo della Digital Transformation e della Cybersecurity", si legge in un *comunicato* congiunto.
*(source: https://www.startmag.it/innovazione/cybersecurity-leonardo-engineering/ )*

### DEVELOPING A STRONG CYBERSECURITY WORKFORCE: INTRODUCING THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

21 settembre 2022 – The Cybersecurity Skills Conference highlighted the actions taken by ENISA to create a common understanding of the roles, competencies, skills and expert knowledge required to engage in a professional activity in the field and introduced the features of the new European Cybersecurity Skills Framework (ECSF).
*(source: https://www.enisa.europa.eu/news/developing-a-strong-cybersecurity-workforce-introducing-the-european-cybersecurity-skills-framework )*

### CYBERSECURITY IN SANITÀ, GLI ATTACCHI IMPATTANO SULLA QUALITÀ DELL'ASSISTENZA

19 settembre 2022 – C'è un legame diretto tra gli attacchi informatici subiti dalle strutture sanitarie e le condizioni dei pazienti che si affidano alle loro cure. A evidenziarlo è una recente ricerca realizzata da ***Ponemon Institute*** con la società di ***sicurezza informatica*** ***Proofpoint***, "**Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care**", che ha coinvolto 641 professionisti dell'It e della sicurezza sanitaria.
*(source: https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-in-sanita-gli-attacchi-impattano-sulla-qualita-dellassistenza/ )*

### L'EMERGENZA DEL FUTURO: COSÌ I PARTITI SI SONO DIMENTICATI DELLA CYBERSICUREZZA

21 settembre 2022 – È un argomento spesso dimenticato dalla politica e che, oltretutto, fatica ad appassionare. Ultimamente

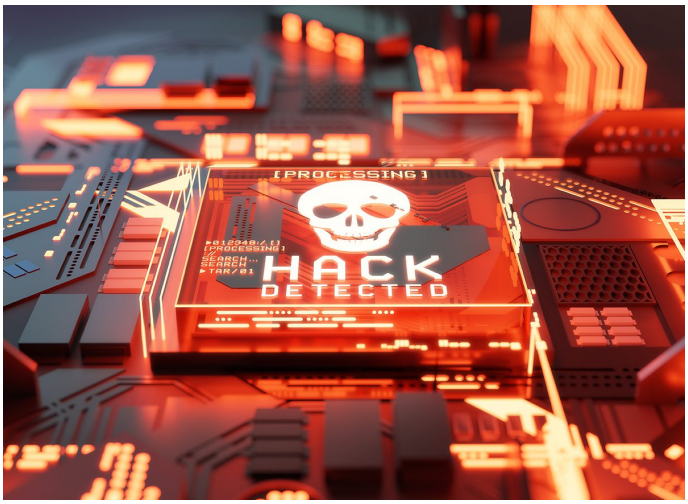
però sulla Cybersecurity sembra che qualcosa stia cambiando. In questi anni è diventato sempre più evidente che i crimini informatici non solo sono qui per rimanere, ma stanno anche aumentando. Durante la pandemia di ***Covid-19*** e dopo l'invasione russa dell'Ucraina, la cybersicurezza si è spesso guadagnata i riflettori come dimensione ineliminabile per la cura, lo sviluppo e la tutela degli interessi italiani.
*(source: https://www.tpi.it/politica/partiti-dimentica-cybersicurezza-campagna-elettorale-20220921932507/ )*

## CYBERSECURITY, SUPPLY CHAIN NEL MIRINO DEI RANSOMWARE: COLPITE 6 AZIENDE SU 10

22 settembre 2022 – I dati Trend Micro sull'ultimo triennio: solo il 51% delle vittime condivide con i fornitori i dati sulle offensive subite, e il 37% non informa i partner sulle minacce. L'Head of Sales Alessandro Fontana: "Serve più visibilità sulla superficie di attacco digitale".
*(source: https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-supply-chain-a-rischio-ransomware-colpite-6-aziende-su-10/ )*

## SICUREZZA INFORMATICA, COME INDIVIDUARE I PUNTI DEBOLI

23 settembre 2022 – Il progetto realizzato da **Unguess** dal titolo *Caso Milkman Technologies: cybersecurity made in the crowd* (risultato finalista ai *Digital Awards* 2022 per la categoria **Information e Cyber Security**) aveva l'obiettivo di analizzare il livello di sicurezza dell'ecosistema digitale dell'azienda cliente per individuare eventuali punti deboli e criticità.
*(source: https://www.zerounoweb.it/techtarget/searchsecurity/cybersecurity/sicurezza-informatica-come-individuare-i-punti-deboli/ )*




## WINDOWS 11, LA NUOVA SECURITY BASELINE CON L'AGGIORNAMENTO 22H2: COS'È E COME ATTIVARLA

23 settembre 2022 – Con l'aggiornamento 22H2 di Windows 11 Microsoft ha reso disponibile anche la nuova security baseline: un insieme di impostazioni granulari di configurazione consigliate e preconfigurate che possono essere testate e personalizzate per adeguarle alla propria organizzazione. Ecco tutto quello che c'è da sapere.
*(source: https://www.cybersecurity360.it/soluzioni-aziendali/windows-11-la-nuova-security-baseline-con-laggiornamento-22h2-cose-e-come-attivarla/ )*

## GLI SVILUPPATORI DI MALWARE AMANO RUST. E SAPERLO CI AIUTERÀ A DIFENDERCI

21 settembre 2022 – Comprendere i *malware*, a basso livello, passa sempre per l'analisi del loro codice. E sebbene occorra effettuare del *reverse engineering* per venire a capo del loro funzionamento, in molti casi è utile conoscere il linguaggio di programmazione coi quali sono stati realizzati. **Per svariati motivi: uno dei principali è che il linguaggio, spesso, definisce il modo in cui un software gestisce la memoria**, sfrutta o meno delle librerie e, in genere, come si comporta e come potrà essere aggiornato e potenziato.
*(source: https://www.cybersecurity360.it/cybersecurity-nazionale/gli-sviluppatori-di-malware-amano-rust-e-saperlo-ci-aiutera-a-difenderci/ )*

## CYBERSECURITY, COME LE BANCHE POSSONO (E DEVONO) ATTREZZARSI

23 settembre 2022 – La minaccia della cybersicurezza non è una novità per il settore finanziario e bancario, ma l'inizio del conflitto (economico e politico) con la Russia ha improvvisamente aumentato l'attenzione delle amministrazioni bancarie sulla **difesa dei propri sistemi informatici**.
È proprio su quest'argomento che si è concentrato una delle conferenze del **Banking Summit organizzato dall'Innovation Group** il 22 e 23 settembre, con diversi protagonisti del settore finanziario e specialisti di sicurezza informatica.
*(source: https://www.we-wealth.com/news/fintech/digital-transformation/cybersecurity-come-le-banche-possono-e-devono-rispondere )*

## CYBERSECURITY: ESCALATION RUSSIA, RISCHIO CYBER SEMPRE PIÙ CONCRETO

23 settembre 2022 – "*Le dichiarazioni odierne del Vice Capo del Consiglio di Sicurezza della Federazione Russa, Dmitry Medvedev, rendono sempre più concreto il rischio di un confronto ostile anche sul piano cyber*", sottolinea Pierguido Iezzi, CEO di Swascan, società parte del polo cyber di Tinexta.
"*L'utilizzo di qualsiasi arma per la propria difesa* – come ha detto Medvedev – *implica per forza di cose l'estensione del fronte sul piano digitale, che non a caso viene definito la quinta dimensione della guerra. Ciò comporterà tre distinte ricadute in tre ambiti differenti: quello prettamente militare, quello geopolitico e quello sociale*".
*(source: https://www.reportdifesa.it/cybersecurity-escalation-russia-rischio-cyber-sempre-piu-concreto/ )*

## LA CYBERSECURITY AWARENESS

23 settembre 2022 – Essere consapevoli dell'esistenza di un pericolo e delle conseguenze che questo comporta, rappresenta il primo strumento di difesa.
La cybersecurity awareness trasforma i dipendenti nella prima linea di difesa contro il cyber crime, sensibilizzandoli, rendendoli consapevoli circa le tipologie, i metodi e gli impatti degli attacchi cyber ai danni di computer, server, reti, dispositivi mobili e dati aziendali.
Il fine è elevare il livello di sicurezza dell'intera organizzazione, trasformando i comportamenti e migliorando la security posture.
*(source: https://www.analisidifesa.it/2022/09/la-cybersecurity-awareness/ )*

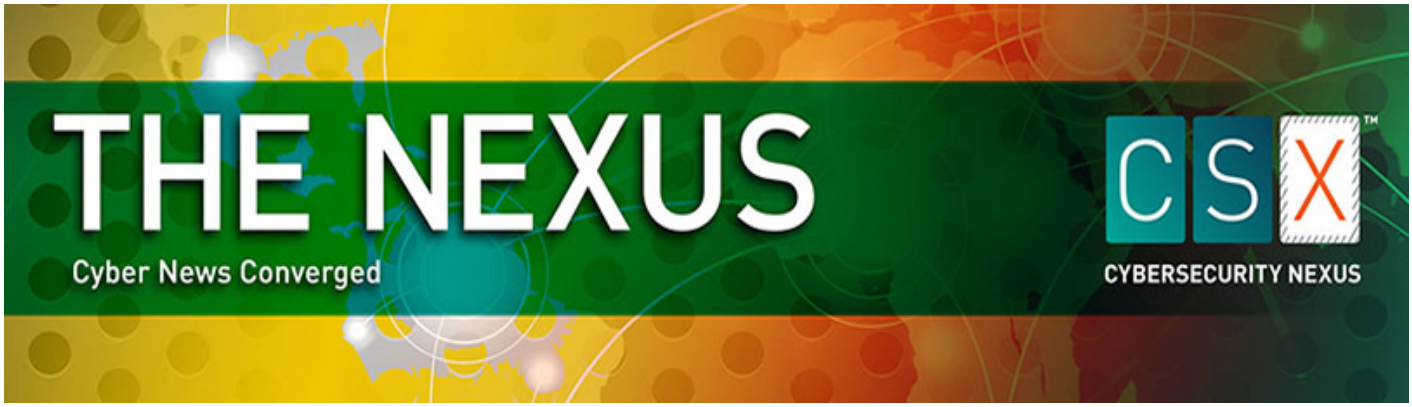
## CORSI ISACA

### L'ATTIVITÀ FORMATIVA DI ISACA ROMA NON È SOSPESA!
### I CORSI SONO EROGATI IN MODALITÀ ONLINE

**LA NUOVA CERTIFICAZIONE CSX-P (CYBERSECURITY PRACTITIONER)**

*Per ulteriori informazioni visitare il sito dedicato alla certificazione CSX-P (www.csxp.it).*

***ULTERIORI INFORMAZIONI SUI CORSI NELLE SEZIONI SPECIFICHE DEL SITO WWW.ISACAROMA.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 ultradecennale 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

Social Media

http://www.isacaroma.it/

SAPIENZA
UNIVERSITÀ DI ROMA

## CISA, CRISC, CISM, CGEIT, CSX-P O CDPSE
## DOPO IL TUO NOME DIMOSTRA CHE HAI LE COMPETENZE PER AFFRONTARE LE SFIDE DELL'AZIENDA MODERNA:

**GET CERTIFIED**


Info al sito *https://www.isaca.org/credentialing/*