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

Newsletter

ANNO 2022 | N. 9 | OTTOBRE

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

AGGIORNAMENTO SULLE MINACCE INFORMATICHE

Lo scenario delle minacce digitali è continuamente mutevole, con sfide sempre crescenti legate al progressivo incremento del numero e della qualità malevola degli "oggetti" di attacco. Gli ultimi report di sicurezza hanno evidenziato nuove tipologie di malware e fornito le ultime classifiche dell'incidenza.

Secondo i ricercatori Check Point il numero degli attacchi è cresciuto del 59% rispetto allo scorso anno con dati più che raddoppiati: se in Italia, negli ultimi 6 mesi, un'organizzazione è stata attaccata in media 1214 volte a settimana, un'organizzazione a livello globale ha subito in media 1142 attacchi. Nonostante l'attività degli attaccanti sia sempre "molto energica", la 17ma edizione del "*The Global Risks Report 2022 del World Economic Forum* (WEC)" ha evidenziato come il 95% dei problemi di cybersecurity sia causato da errori umani. Sempre il WEC aveva pronosticato una cyberpandemia globale simile al Covid, con una diffusione più veloce e lunga rispetto al virus biologico e con un impatto economico pari o superiore. A valle dei dati sul 2021 è possibile confermare come lo scorso anno si sia assistito a una doppia pandemia: biologica ed informatica.

Conoscere alcune delle evidenze sui nuovi malware permette di istruire appropriate azioni preventive di difesa: **AdvancedIP-Spyware**, apparso in un recente *report sul crimeware* (Fonte Kaspersky), rappresenta una versione con backdoor dello strumento legittimo Advanced IP Scanner, utilizzato dagli amministratori di rete per controllare le reti locali (LAN). Lo strumento dannoso ha colpito un vasto pubblico con aziende vittime in Europa Occidentale, America Latina, Africa, Asia Meridionale, Australia e Paesi della Comunità degli Stati Indipendenti (CSI). Il malware è caratterizzato da un'architettura modulare, aspetto tipico del malware "state sponsored" e non di quello di tipo criminale. Tuttavia, poiché gli attacchi non erano mirati, sembra che AdvancedIPSpyware non faccia riferimento a campagne a sfondo politico.

Dagli stessi ricercatori anche la segnalazione della campagna dannosa ad opera del **malware** ***Obot***, un noto Trojan bancario, in grado di rubare i dati e le e-mail degli utenti dalle reti aziendali infette, di diffondersi ulteriormente nella rete e di installare ransomware o altri Trojan su altri dispositivi della rete. I criminali informatici presumibilmente intercettano le e-mail attive che riguardano conversazioni su questioni di lavoro e inviano ai destinatari un messaggio contenente un link con un file archiviato con una password

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

da scaricare per infettare i loro dispositivi con un trojan bancario. Per convincere gli utenti ad aprire o scaricare il file, gli attaccanti di solito adescano con la promessa di offerte commerciali o la presenza di informazioni importanti. Questo schema rende i messaggi più difficili da individuare e aumenta le probabilità che il destinatario cada nella trappola. La nuova ondata di attività ha causato oltre 1.500 utenti colpiti a partire dal 28 settembre 2022. Tra i Paesi più attaccati ci sono gli Stati Uniti con 193 utenti, seguiti da Italia con 151, Germania con 93 e India con 74 (al 4 ottobre 2022). Sono stati scoperti più di 400 siti web infetti che diffondono Qbot. La particolare pericolosità delle mail di phishing che diffondono il trojan risiede nell'imitazione della corrispondenza di lavoro come trucco comune usato dai criminali informatici, o l'intercettazione di una conversazione esistente della vittima target inserendosi nella corrispondenza. Tale metodo rende questi messaggi molto più difficili da individuare e aumenta le probabilità che il destinatario apra i file. Si suggerisce di prestare una continua attenzione e cautela, per evitare di aprire accidentalmente un file dannoso contenente Qbot.

HydraPoS e AbanddonPoS sono le famiglie di malware più diffuse nel 2022 e rappresentano circa il 71% di tutti i casi di attacchi ai sistemi di pagamento PoS, mentre per gli ATM il malware più attivo è **Ploutus,** che rappresenta il 3% di tutti i rilevamenti di malware di POS nei primi otto mesi del 2022. Il motivo della recrudescenza di queste minacce rivolta ad asset fisici risiede nel ritorno all'uso dei metodi di pagamento tradizionali svolti "in presenza" e di conseguenza l'attività dei criminali informatici si sta intensificando. I criminali informatici attaccano i sistemi integrati di sportelli bancomat e terminali PoS per rubare contanti, credenziali delle carte di credito e dati personali, e penetrano nei sistemi per ottenere il controllo di tutti i dispositivi all'interno di una rete; gli attaccanti possono ottenere migliaia di dollari in una notte. Nel 2021, il numero di dispositivi colpiti da malware ATM/PoS è aumentato del 39% rispetto all'anno precedente. Nei primi otto mesi del 2022, il numero è cresciuto del 19% rispetto allo stesso periodo del 2020 e di quasi il 4% rispetto al 2021. (Fonte *report sul malware per ATM/PoS*)

Sul fronte delle **minacce scaturite dalla contrapposizione Russo/Ucraina** tra febbraio e agosto di quest'anno sono stati riscontrati attacchi più che raddoppiati al governo e al settore militare dell'Ucraina con un aumento del 112%, mentre lo stesso settore della Russia è diminuito dell'8% ed in particolare (Fonte Cheeck Point): sono stati contati oltre 1.500 attacchi informatici settimanali in media su ogni rete aziendale in Ucraina, un numero superiore alla media globale (1.124 attacchi informatici settimanali) e alla Russia (1.434 attacchi informatici settimanali); è stato rilevato un aumento del 25% della media settimanale di attacchi informatici alle reti aziendali in Ucraina, rispetto all'inizio dell'anno prima del conflitto, mentre a livello mondiale l'aumento è stato dello 0,1% e in Russia del 13% (solo reti aziendali). Parte degli attacchi è stata causata da **Killnet un gruppo di hacktivisti orientato ad attaccare i paesi ritenuti "ostili" alla Russia.** Originariamente dediti a ai servizi di "DDoS a noleggio" dal gennaio 2022, il gruppo Killnet è, di fatto, un gruppo di criminali informatici che tra marzo e settembre 2022, ha acquisito notorietà a mezzo dell'uso di ransomware prendendo di mira organizzazioni all'interno di paesi che hanno sostenuto l'Ucraina o hanno intrapreso azioni ritenute dannose per gli interessi della Russia (Fonte *CSA.org*). Sergey Shykevich, Threat Intelligence Group Manager di Check Point spiega che "il punto di forza di Killnet risiede nella determinazione verso i bersagli: si concentrano sui siti web più importanti del governo federale (riferito ai recenti attacchi in terra americana n.d.r.) e su quei siti web per i quali non si possono ignorare tempi di inattività significativi, ma che non sono sufficientemente protetti".

Due ambiti molto gettonati dagli attaccanti anche prima della pandemia e della guerra sono stati i **settori del gaming e quello della sanità**: la pandemia ha accresciuto il gaming online come sbocco necessario per l'intrattenimento e l'interazione sociale e creazione di centinaia di migliaia di nuovi account ha favorito la nascita e proliferazione di nuove community che abilitano l'interazione fra i gamer attraverso call o messaggi istantanei durante le partite. In Italia, secondo il Rapporto Annuale di IIDEA (Italian Interactive Digital Entertainment Association) il 2021 ha fatto registrare un giro d'affari di 2

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

miliardi e 243 milioni di euro, in crescita del +2,9% rispetto al 2020 con un numero di gamer pari a circa 15,5 milioni di persone. Il gaming è un mercato in continuo sviluppo sia in termini di fatturato che di partecipanti e questi elementi "ingolosiscono" i criminali digitali per la platea di "potenziali vittime". I gamer sono interessanti per i criminali per vendere gli asset virtuali in cambio di denaro reale; rubare direttamente i giochi, ottenere più informazioni possibili per furti di identità e frodi bancarie.

In ambito sanitario è invece il ransomware che ha costretto un'organizzazione su quattro a fermare le operazioni in seguito a un attacco, con conseguenze che possono inficiare sulla vita dei pazienti. Il dato emerge da EVERYTHING IS CONNECTED: Uncovering the ransomware threat from global supply chains, l'ultima ricerca Trend Micro. Lo studio mostra come Il 57% delle organizzazioni sanitarie di tutto il mondo abbia ammesso di essere stato compromesso da un ransomware negli ultimi tre anni. Delle organizzazioni colpite, il 25% è stato costretto a interrompere completamente le operazioni, mentre il 60% ha subito modifiche nei processi aziendali. Il 60% del campione ha ammesso di aver subito il furto di dati sensibili, aumentando così i rischi alla conformità, i danni reputazionali, i costi di indagine, riparazione e pulizia. La maggior parte (il 95%) dei responsabili delle organizzazioni sanitarie aggiorna regolarmente le patch, mentre il 91% ha impostato delle limitazioni agli allegati e-mail per mitigare il rischio malware. Molti usano anche strumenti di rilevamento e risposta per gli endpoint (Endpoint Detection & Respond - EDR), le reti (Network Detection & Response -NDR) e su più livelli (eXtended Detection & Response - XDR), ma restano alcuni punti deboli: un quinto (17%) non dispone di alcun controllo del protocollo (Remote Desktop Protocol-RDP); molte organizzazioni sanitarie non condividono alcuna intelligence sulle minacce con i partner (30%), i fornitori (46%) o il loro ecosistema più ampio (46%); un terzo (33%) non condivide alcuna informazione con le Forze dell'Ordine; solo la metà o un numero inferiore di Organizzazioni Sanitarie attualmente utilizza strumenti NDR (51%), EDR (50%) o XDR (43%); pochi intervistati sono in grado di rilevare il movimento laterale (32%), l'accesso iniziale (42%) o l'uso di strumenti come Mimikatz e PsExec (46%).

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!

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

EVENTI PASSATI

GIOV 27 OTTOBRE 2022

ORE 15:00-18:30

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

Il webinar ha illustrato 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.***

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.

Gli annunci e gli inviti saranno spediti con le consuete modalità agli iscritti alla nostra mai-ling list.

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

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

LE PRINCIPALI NOTIZIE

AGENZIA CYBERSECURITY: VIA A CONCORSO PER ASSUNZIONE 60 RISORSE

31 ottobre 2022 – Contratti a tempo indeterminato. Sette i profili richiesti con esperienza post diploma di almeno tre anni. Candidature fino al 28 novembre. Il direttore Baldoni: "Cerchiamo i migliori tecnici che vogliano impegnare il proprio talento e le proprie competenze al servizio dell'interesse del Paese"
(source: https://www.corrierecomunicazioni.it/cyber-security/agenzia-cybersecurity-via-a-concorso-per-assunzione-60-risorse/)

WHAT IS A DATA BREACH AND HOW TO PREVENT IT

31 ottobre 2022 – A data breach is a cybersecurity incident where someone accesses a system to view or copy sensitive or private information without authorization. Hackers can infiltrate an organization by taking advantage of human error, but some are skilled enough to break even the most secure systems. A single data breach can impact a massive amount of people — for example, Yahoo's three billion user accounts — and/or have long-lasting consequences when the information released is highly sensitive, like in the 2017 Equifax breach.
Once the data is out on the web, it's hard to put the toothpaste back in the tub. As a result, companies that suffer a breach will often offer free credit monitoring services for affected customers, which contributes to the overall cost of data breaches.
(source: https://money.com/what-is-a-data-breach/)

PUBBLICATA LA ISO/IEC 27001:2022. UNA NUOVA ERA PER LA SICUREZZA DELLE INFORMAZIONI

26 ottobre 2022 – La nuova versione dello standard ISO 27001 aiuta le organizzazioni a gestire i controlli in modo più efficace raggruppandoli in quattro "temi" chiari: organizzativo, personale, tecnologico e fisico. Questo cambiamento chiave mira a ottenere maggiore chiarezza, attenzione e responsabilità per la sicurezza delle informazioni all'interno di un'organizzazione.
Lo standard presenta anche i controlli di sicurezza delle informazioni recentemente aggiornati delineati dalla ISO 27002:2022, che rappresentano la revisione più significativa. Ora ci sono 93 controlli invece di 114; 11 sono nuove aggiunte, mentre altre sono state unite o rimosse.
(source: https://www.cybersecitalia.it/pubblicata-la-iso-iec-270012022-una-nuova-era-per-la-sicurezza-delle-informazioni/21625/)

INTELLIGENZA ARTIFICIALE SHOCK: DI FATTO SIETE SEMPRE SPIATI | 1984 NON È PIÙ SOLO UN ROMANZO

31 ottobre 2022 – **Fino a dove si può spingere l'intelligenza artificiale e quanto ancora non sappiamo delle sue infinite possibilità? La verità potrebbe sorprendervi non poco.**
Uno degli aspetti più interessanti del Novecento è stato il **rapporto dell'uomo con le "macchine"**. La tecnologia, infatti, cominciava a muovere i suoi rudimentali, ma giganti, passi verso un mondo nuovo, molto più veloce di noi umani e questa previsione del futuro, collegata alla paura dei sistemi politici più autoritari che hanno caratterizzato il secolo breve, hanno dato il via agli immaginari più distopici.
(source: https://www.newnotizie.it/2022/10/31/intelligenza-artificiale-shock-di-fatto-siete-sempre-spiati-1984-non-e-piu-solo-un-romanzo/)

LA CYBERSECURITY PUNTA SUL "AS A SERVICE"

31 ottobre 2022 – Il mondo della sicurezza informatica si sta rapidamente evolvendo e sta diventando sempre più complesso. L'approccio necessario per contrastare gli attacchi deve cambiare attraverso un paradigma che punti sulla disponibilità di competenze che non tutte le organizzazioni possono gestire internamente.
(source: https://www.enisa.europa.eu/news/developing-a-strong-cybersecurity-workforce-introducing-the-european-cybersecurity-skills-framework)

CYBERCRIME, 25 CAMPAGNE CONTRO L'ITALIA LA SCORSA SETTIMANA

31 ottobre 2022 – L'Italia è stata presa di mira da 25 campagne del cybercrime. Gli esperti di cybersecurity del CERT-AgID rilevano 8 malware: Lokibot, AgentTesla, Quakbot, Brata, Formbook, IcedID, ASTesla e un payload sconosciuto. Il phishing punta alle PEC
(source: https://www.difesaesicurezza.com/cyber/cybercrime-25-campagne-contro-italia-la-scorsa-settimana/)

LA NUOVA STRATEGIA DI SICUREZZA NAZIONALE USA E L'ASIA

25 ottobre 2022 – La nuova strategia di sicurezza nazionale degli Stati Uniti: quattro spunti per la politica asiatica. La continua enfasi sull'Indo-Pacifico e sulla Cina in tutto l'NSS sembra essere un segnale che se anche gli USA continueranno a mobilitare sostegno all'Europa, non permetteranno che altre crisi facciano deragliare la priorità strategica dell'Indo-Pacifico e la concorrenza con la Cina.
(source: https://lindro.it/la-nuova-strategia-di-sicurezza-nazionale-usa-e-l-asia/)

INTELLIGENZA ARTIFICIALE GENERATIVA: LE APPLICAZIONI

29 ottobre 2022 – C'è una nuova buzzword che sta galvanizzando l'attenzione della Silicon Valley "Generative AI". Col

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

termine Intelligenza Artificiale generativa ci si riferisce all'utilizzo di tecniche di machine learning e deep learning per generare contenuti nuovi sulla base di dati pregressi. In particolare, parliamo dell'utilizzo di modelli linguistici di grandi dimensioni (Large Language Models) che permettono di ottenere testi, immagini, video, codice inedito a partire da un input testuale.
(source: https://vincos.it/2022/10/29/intelligenza-artificiale-generativa-le-applicazioni/)

LO STATO DELL'ARTE DELLA CYBERSECURITY IN EDIZIONE 'STREAMING' A SECURITY SUMMIT 2022

28 ottobre 2022 – La **digitalizzazione** e la riorganizzazione di imprese e pubblica amministrazione in tempo di pandemia, il conflitto europeo, i crescenti fenomeni di **hacktivism ed il cyber crime,** che assume connotazioni sempre più tipiche della criminalità organizzata: questi gli elementi principali che certamente hanno segnato l'andamento degli attacchi informatici nella prima parte dell'anno, determinandone quantità, direzione e gravità.
(source: https://automazione-plus.it/lo-stato-dellarte-della-cybersecurity-in-edizione-streaming-a-security-summit-2022_141597/)

CYBERSECURITY REPORT DI EXPRIVIA: NEL PERIODO ESTIVO CALANO I REATI INFORMATICI

28 ottobre 2022 – In Italia i crimini informatici sembrano rallentare, nel periodo estivo il numero degli attacchi informatici è diminuito rispetto al periodo invernale e si allarga la forbice tra i tentativi e gli incidenti andati a buon fine. È quanto è emerso dal report prodotto dall'Osservatorio Cybersecurity di Exprivia presentato nella giornata conclusiva dell'Apulia Cybersecurity Forum. Se i crimini sono diminuiti nell'ultimo periodo, tuttavia, la situazione non è del tutto positiva.
Video al seguente link: *https://youtu.be/65uVxozTNWw*
(source: https://www.trmtv.it/tecnologia/2022_10_28/350246.html)

COS'È LA KILL CHAIN E COME PUÒ ESSERE UTILE NELLA CYBERSECURITY

28 ottobre 2022 – Il concetto di **Kill Chain** permette di far comprendere e quindi identificare i vari passaggi necessari all'esecuzione di un attacco hacker e far comprendere come un "attaccante", per raggiungere il suo obiettivo debba riuscire a progredire attraverso tutta la catena.
In questa nuova puntata di "**Crypto ma non troppo**", **Donatella Maisto** racconta cos'è la Kill Chain e come può essere utile nel trattare la Cybersecurity.
(source: https://quifinanza.it/green/kill-chain-cybersecurity/673821/)

BALDONI: "ECCO COSA FARÀ NEL 2023 L'AGENZIA DELLA CYBER, PER UNA ITALIA PIÙ PROTETTA"

27 ottobre 2022 – Cercherò di dare alcuni punti essenziali per quanto riguarda quello che è stato fatto in quest'anno, fin quindi fino praticamente a fine settembre. **E quello che dovremmo fare nel 2023 in poi e anche cercare di far capire quali sono le minacce più importanti per quanto riguarda il nostro paese.** Quest'anno è stato l'anno della costituzione dell'***Agenzia per la cybersecurity nazionale.*** Noi di fatto abbiamo avuto i decreti, i regolamenti diciamo di attuazione dell'Agenzia, pubblicati il 27 dicembre dell'anno scorso, quindi siamo in una fase di crescita molto forte.
(source: https://www.cybersecurity360.it/cybersecurity-nazionale/baldoni-ecco-cosa-fara-nel-2023-lagenzia-della-cyber-per-una-italia-piu-protetta/)

UN NUOVO AD PER AICOMPLY: CLAUDIO CILLI

19 ottobre 2022 – E' a partire dal mese di ottobre che Claudio Cilli ha assunto l'incarico di Amministratore Delegato di AiComply, società di Consulting del Gruppo Agic, specializzata nel supporto alle imprese in ambito GRC (Governance, Risk & Compliance) e Consulenza Organizzativa. Ingegnere elettronico e Dottore di Ricerca in Sicurezza Informatica presso l'Università La Sapienza, Cilli è un'autorità riconosciuta a livello internazionale nelle aree della Sicurezza dei Sistemi Informativi, attualmente advisor di Governi e grandi aziende per la cybersecurity e protezione delle infrastrutture critiche. Prima di entrare in AiComply Claudio ha sviluppato una lunga esperienza professionale ricoprendo incarichi e ruoli di responsabilità in grandi realtà della Consulenza Direzionale ed IT.
(source: https://www.techcompany360.it/news/un-nuovo-ad-per-aicomply-claudio-cilli/)

MELONI: "TRANSIZIONE DIGITALE CON SOVRANITÀ TECNOLOGICA E CYBERSECURITY"

25 ottobre 2022 – ***Nel discorso per chiedere la fiducia al Parlamento, la premier pone al centro dell'attività del Governo anche la sicurezza informatica, che deve andare di pari passo "con la transizione digitale, la sovranità tecnologica e il cloud nazionale". Ma come, concretamente?***
Anche la sicurezza informatica al centro delle dichiarazioni programmatiche di ***Giorgia Meloni*** al Parlamento per chiedere la fiducia per il suo governo. La cybersecurity è stata citata una sola volta dalla premier, invece, non lo fece **Mario Draghi** nel suo discorso di insediamento, ma poi con il suo governo è stata istituita l'Agenzia per la Cybersicurezza Nazionale (**ACN**) e ridefinita la governance nazionale in materia di cyber.
(source: https://www.cybersecitalia.it/meloni-transizione-digitale-con-sovranita-tecnologica-e-cybersecurity/21615/)

LE OTTO URGENZE CYBER SECURITY DEL GOVERNO MELONI

18 ottobre 2022 – Alcuni temi della cyber security sono urgenti in Italia e richiedono l'immediata attenzione del nuovo Governo. Ecco una lista. Bisogna tra l'altro proseguire con l'attuazione della strategia cybersecurity con l'Agenzia al centro, ma anche potenziare le partnership pubblico-private e accompagnare enti e pmi alla cyber.
(source: https://www.agendadigitale.eu/sicurezza/le-otto-urgenze-cyber-security-del-governo-meloni/)

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

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 dell'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

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in 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:

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

Questa Newsletter è indirizzata ai soci del Capitolo di Roma di ISACA e viene anche spedita alle persone che hanno chiesto di essere inseriti nella mailing list per la comunicazione degli eventi del Capitolo.
Potete indirizzare ogni vostra richiesta (commenti, contributi, cancellazione dalla lista, ecc.) a newsletter<at>isacaroma.it.
La redazione della Newsletter è curata da Mario Taddonio (membro del CD di ISACA Roma) m.taddonio<at>isacaroma.it e da Glauco Bertocchi (VicePresidente di ISACA Roma) g.bertocchi<at>isacaroma.it
Le opinioni espresse (editoriale, ecc.) rappresentano quelle dei rispettivi autori.

ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.