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

Newsletter

ANNO 2023 | N. 3 | MARZO

ISACA (Information Systems Audit and Control Association)

L'ISACA, (Information Systems Audit and Control Association), ha 160.296 associati in oltre 188 nazioni (dato aggiornato al 31 ottobre 2022) 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

DIFESA DALLA MINACCIA DELL'AIKIDO WIPER

Si scrive AikidoWiper ma si legge minaccia ai sistemi EDR, molto diffusi sul mercato e spesso considerati una difesa necessaria e sufficiente al suo scopo. Vedremo che non è proprio così, a riprova che qualsiasi tool di sicurezza può esso stesso trasformarsi in un target di attacco.

La storia di questa minaccia inizia all'evento Backhat 2022 in cui Or Yar un ricercatore dei Safebreach Labs ha presentato una vulnerabilità 0-day presente su 6 degli 11 strumenti di Endopoint Detection & Response (EDR) da lui testati, ovvero sui seguenti: Microsoft Windows Defender, Windows Defender for Endpoint, TrendMicro ApexOne, Avast Antivirus, AVG Antivirus e SentinelOne. La vulnerabilità offre agli aggressori un modo per manipolare i prodotti in modo da cancellare praticamente tutti i dati sui sistemi installati. Per dimostrare come la vulnerabilità potesse essere sfruttata il ricercatore ha creato un tool, denominato AIKIDO WIPER rendendolo disponibile su Github. Il tool costringe la soluzione EDR a cancellare i file di sistema per conto di un utente non privilegiato, rendendo i sistemi non più attivabili con conseguenze critiche di operatività, danni economici e reputazionali. L'exploit Aikido Wiper è un esempio di come un avversario usi la forza del sistema di difesa contro sé stesso, proprio come con l'arte marziale dell'Aikido opera nello sfruttare la forza dell'avversario per difendersi. Ma in questo caso si usa la forza del sistema di difesa per attaccarlo meglio. Infatti, i prodotti di sicurezza, come gli strumenti EDR, hanno diritti di superutente e un avversario in grado di abusarne può eseguire attacchi in modo praticamente non rilevabile.

Oltre ad essere uno 0-day, la notizia significativa è stata che la tecnica proposta da Or non ha bisogno di utenze privilegiate per funzionare. Solitamente infatti per la violazione degli endpoint, gli attaccanti cercano di violare il sistema di gestione delle identità, tipicamente tramite sfruttamento di Attack Path sull'Active Directory, scalando le identità ed appropriandosi di una utenza di tipo privilegiato. Questo anche per manipolare, esfiltrare i dati o per studiare la rete partendo dall'endpoint come punto di appoggio. Ma se l'obiettivo è interrompere l'operatività di un particolare device ed utente, allora questo wiper dimostra che gli basta una utenza qualunque (per approfondimenti sulla tecnica si veda il paper di Or Yar o l'analisi di Darkreading).

La tecnica rientra nella più ampia casistica del wiperware, che sono pseudo ransomware con l'unico obiettivo di distruggere i sistemi della vittima, piuttosto che offrire l'opportunità di de-crittografarli dietro pagamento di un riscatto. Questa forma di attacco informatico è spesso di natura geopolitica e differisce dalla maggior parte degli odierni attori ransomware, motivati finanziariamente, che utilizzano tattiche come la doppia estorsione per ottenere un riscatto. Nel caso dei recenti attacchi informatici all'Ucraina, gli aggressori hanno mantenuto un ping aperto fino

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

a quando non hanno eliminato tutti i file potenzialmente utili sull'host con un'ultima fase di pulizia. I messaggi presentati dal wiperware tendono a fungere da meccanismi di ritardo per le indagini di ripristino man mano che viene determinato l'impatto.

Dalla scoperta della vulnerabilità che Or ha effettuato a Luglio-Agosto 2022, e presentata a dicembre nel rispetto della pratica di Coordinated Vulnerability Disclosure (CVD), tre dei fornitori hanno assegnato numeri CVE formali per i bug e rilasciato patch. Le CVE sono: **Microsoft:** CVE-2022-37971, **TrendMicro:** CVE-2022-45797, **Avast & AVG:** CVE-2022-4173. Le corrispondenti versioni corrette dei prodotti invece sono **Microsoft Malware Protection Engine:** 1.1.19700.2, **TrendMicro Apex One:** Hotfix 23573 & Patch_b11136, **Avast & AVG Antivirus:** 22.10. Ricordiamo che la CVD è il modello in cui una vulnerabilità o un problema viene divulgato al pubblico solo dopo che alle parti responsabili è stato concesso un tempo sufficiente per riparare o porre rimedio alla vulnerabilità o al problema. Questo coordinamento distingue il modello CVD dal modello "full disclosure" che evidentemente avvantaggia gli avversari malevoli.

Per avviare difese efficaci ed efficienti oltre naturalmente ad installare le patch rese disponibili dai vendor dei singoli EDR, si rende necessario ricorrere alla difesa multilivello, come una "cipolla", in cui l'EDR rappresenta un livello esterno mentre la sicurezza basata sull'identità è al centro del sistema. Questo perché, se si considera che i malintenzionati abbiano già violato il proprio ambiente, allora bisogna supporre che, una volta entrati, non intendano cancellare i dati su tutti i computer, ma anche impadronirsi dell'Active Directory per accedere a risorse ancora più cruciali presenti nell'ambiente. In questi casi un piano di recovery costituisce una solida soluzione, a patto di includere tutti i sistemi critici e l'intera foresta di Active Directory (o gli equivalenti sistemi di gestione identità per gli altri sistemi operativi).

Tre i principi fondamentali quindi: evitare il "single point of failure", avere un piano di recovery, e monitorare la rete interna, ma anche l'avversario. Ecco su quest'ultimo punto torniamo alla dinamica propria dell'Aikido come arte marziale: studiare e conoscere il proprio avversario significa saper sfruttare la sua forza a proprio vantaggio. E quindi è sempre importante avere analisi di intelligence, threat model degli avversari considerati più propensi ad attaccare la propria organizzazione. Il suggerimento è quello di mantenere aggiornato un modello della minaccia e degli attori malevoli, delle tecniche e tattiche (si ricorda il *MITRE ATT&CK framework* come punto di partenza n.d.r.) altrimenti all'equazione della difesa manca un addendo fondamentale che impedisce di vedere o se preferite, di intuire, i potenziali punti di attacco e attuare una difesa puntuale e preventiva per ognuno.

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

VENERDÌ 24 MARZO 2023
15:00-17:00 (2 CPE)

"L'IMPORTANZA DELLA FORMAZIONE NELLA PROTEZIONE DEI DATI PERSONALI. Un esempio di formazione per la filiale bancaria"

L'obbligo di formazione (artt. 29 e 32 del GDPR) delle persone autorizzate al trattamento riveste, come peraltro nella previgente normativa, grande importanza nella protezione dei dati personali ed è posta oggi anche sotto la sorveglianza del DPO [art. 39 c. 1 lettera b) del GDPR]. Appare però necessario che tale formazione verta in particolar modo sui trattamenti effettivamente svolti dalle diverse unità organizzative in cui è articolata l'azienda. Si presenta un esempio di seminario orientato al personale che opera in una filiale bancaria.

Indice dell'intervento:

1. Importanza della formazione nella data protection: gli obblighi derivanti dal GDPR e da altri provvedimenti del Garante privacy.
2. Il ruolo del DPO e la relazione con la formazione sulla cybersecurity .
3. Un esempio concreto: la formazione per una filiale bancaria
    a. Inquadramento normativo e definizioni
    b. I principali adempimenti svolti in filiale: resa della informativa e raccolta del consenso.

Problematiche connesse: esercizio dei diritti da parte della clientela, marketing, accesso a dati bancari della clientela, disciplina delle comunicazioni alla clientela .

Relatore: ***Dott. Cesare Maria De Santis Puzzonia***

Ha lavorato per diverse aziende ed Enti - Ispettorato Telecomunicazioni e Assistenza al Volo dell'A.M., Ispettorato Logistico dell'A.M., Banca Nazionale del Lavoro, Ipacri SpA (Club sul Computer Crime), Istinform SpA, Euros Consulting SpA ed OASI SpA - prima di intraprendere un autonomo percorso professionale. Attualmente è amministratore unico di PRIMAe srl, società di consulenza operante sul tema della protezione dei dati personali ed è in possesso della certificazione CISM (Certified Information Security Manger) di ISACA ed iscritto altresì nel registro "Data Protection Officer", in accordo alla norma UNI 11697:2017, di KHC. Tra i clienti di PRIMAe srl si annoverano diverse società finanziarie e banche in alcune delle quali svolge il servizio DPO.

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 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

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

LE PRINCIPALI NOTIZIE

AIKIDO WIPER MANIPOLA GLI ANTIVIRUS PER CANCELLARE FILE ANCHE SENZA PERMESSI PRIVILEGIATI: COME DIFENDERSI

27 dicembre 2022 – Aikido Wiper è un nuovo malware in grado di compromettere i software di sicurezza installati sui sistemi target per renderli inaccessibili cancellando file e cartelle. Ecco quali insegnamenti devono trarre le organizzazioni da questa scoperta e come proteggere le proprie infrastrutture.
(source: https://www.cybersecurity360.it/nuove-minacce/aikido-wiper-manipola-gli-antivirus-per-cancellare-file-anche-senza-permessi-privilegiati-come-difendersi/)

GUERRA RUSSIA-UCRAINA: SI PUÒ PARLARE DI CYBERWAR? IL PUNTO A UN ANNO DALL'INIZIO DEL CONFLITTO

02 marzo – E' ormai trascorso **un anno dall'invasione dell'Ucraina da parte della Russia** e, da quel momento, molto spesso si è sentito parlare di *cyberwar*. Infatti, sono state numerose le voci che hanno ritenuto che fosse arrivato il momento in cui i conflitti si sarebbero spostati nel **dominio cibernetico**.

Eppure, se si analizza in maniera lucida lo scontro attuale, emerge che, fino ad oggi, **lo strumento informatico ha ricoperto un ruolo esclusivamente ancillare**. Infatti, è stato **largamente utilizzato dalla Russia nelle fasi preliminari all'invasione** come mezzo di pressione psicologica sulla popolazione ucraina, mentre, durante il conflitto, vi è stata una netta prevalenza delle armi tradizionali.
(source: https://www.cybersecurity360.it/nuove-minacce/guerra-russia-ucraina-si-puo-parlare-di-cyberwar-il-punto-a-un-anno-dallinizio-del-conflitto/)

FERRARI DISCLOSES DATA BREACH AFTER RECEIVING RANSOM DEMAND

20 marzo – Ferrari has disclosed a data breach following a ransom demand received after attackers gained access to some of the company's IT systems.
"We regret to inform you of a cyber incident at Ferrari, where a threat actor was able to access a limited number of systems in our IT environment," Ferrari says in breach notification letters sent to customers.
(source: https://www.bleepingcomputer.com/news/security/ferrari-discloses-data-breach-after-receiving-ransom-demand/)

VIAGGIO NELL'INTELLIGENZA ARTIFICIALE: ECCO COME (GIÀ ORA), STA CAMBIANDO IL MODO DI LAVORARE IN UFFICI E AZIENDE

20 marzo – «*ChatGpt* è passato come una cometa in una notte senza luna e ha costretto tutti ad alzare la testa. Com'è stata accolta quest'ondata di attenzione per le cosiddette «intelligenze artificiali generative» da parte di chi già sfrutta questa nuova frontiera tecnologica in concreto? Per capirlo, cominciamo un viaggio dentro le realtà - aziendali o accademiche - che da più o meno tempo lavorano proprio con l'intelligenza artificiale (IA), in ambiti che fino a qualche anno fa erano dominio unico dell'uomo e che oggi non lo sono più. La prima è **Contents.com**, che si occupa (come suggerisce il nome) di creare contenuti a 360 gradi attraverso l'IA.
(source: https://video.corriere.it/tecnologia/viaggio-intelligenza-artificiale-incontriamo-chi-gia-ci-lavora/f635fe0e-c1bb-11ed-839f-35544f562c09)

ChatGPT SUFFERS FIRST DATA BREACH, EXPOSES PERSONAL INFORMATION

24 marzo – OpenAI's ChatGPT has suffered its first major personal data breach.
The breach came during a March 20 outage and exposed payment-related and other personal information of 1.2% of the ChatGPT Plus subscribers who were active during a specific nine-hour window, according to a ***blog post by OpenAI Friday, March 24***.
"In the hours before we took ChatGPT offline on Monday, it was possible for some users to see another active user's first and last name, email address, payment address, the last four digits (only) of a credit card number, and credit card expiration date. Full credit card numbers were not exposed at any time," OpenAI officials wrote today.
(source: https://www.cmswire.com/digital-experience/chatgpt-suffers-first-data-breach-exposes-personal-information/)

GDPR, GLI ERRORI PIÙ COMUNI CHE FANNO SANZIONARE LE AZIENDE

20 marzo – facile notare una azione sempre più incisiva, da parte delle Autorità di Controllo, nel **sanzionare i *titolari del trattamento*** per non aver ottemperato in modo corretto ai doveri previsti dal capo III del GDPR (rubricato: Diritti dell'interessato).
Riassumendoli, i Titolari sono tenuti a:

- **fornire**, agli interessati **tutte le informazioni necessarie** a renderli edotti di come tratteranno i loro dati e di quali sono i loro diritti;
- **agevolare** l'esercizio di tali diritti;
- fornire agli interessati un **riscontro puntuale** rispetto all'azione intrapresa a seguito di una istanza di esercizio dei diritti.

(source: https://www.agendadigitale.eu/sicurezza/privacy/gdpr-che-significa-agevolare-lesercizio-dei-diritti-cosa-sapere-per-evitare-sanzioni/)

QUELLA NORMA CHE SALVA L'EX DIRETTORE DELLA CYBERSICUREZZA

20 marzo – Il Consiglio dei ministri ha nominato il prefetto di Roma, Bruno Frattasi, nuovo direttore dell'Acn – Agenzia per la

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

Cybersicurezza nazionale – dopo le dimissioni di **Roberto Baldoni**. Il nuovo direttore, molto vicino al ministro dell'Interno, Matteo Piantedosi, resterà affiancato dalla vice, Nunzia Ciardi, molto stimata nel settore. Una tecnica competente, infatti, sarà di aiuto al nuovo direttore per la messa a terra in continuità degli ingenti finanziamenti Pnrr, pari a 623 milioni di euro, e della crescita dell'organico dell'agenzia fino a 800 risorse prevista nei prossimi anni.
(source: https://espresso.repubblica.it/opinioni/2023/03/20/news/cybersicurezza_frattesi-392365751/)

CYBERSICUREZZA: COS'È L'ATTACCO DDOS CHE GLI HACKER FILO-RUSSI HANNO SFERRATO AL CSM

19 marzo – NoName057, il gruppo di hacker filorusso, ha rivendicato un nuovo attacco. Vittima dei criminali informatici, questa volta, è il sito del Csm che, sovraccaricato dall'attacco, è stato rallentato a tal punto da rendere impossibile la navigazione. Tecnicamente, il gruppo ha `sferrato´ un attacco *Ddos*. Di cosa si tratta? In sostanza, è un tipo di attacco informatico che tenta di rendere non disponibile un sito web o una risorsa di rete sovraccaricandoli con traffico dannoso e rendendoli di conseguenza inutilizzabili. L'acronimo sta per *Distributed Denial-of-Service*: gli hacker appesantiscono il sito preso di mira con traffico Internet indesiderato, impedendo a quello normale di giungere alla destinazione prevista.
(source: https://www.globalist.it/intelligence/2023/03/19/cybersicurezza-cose-lattacco-ddos-che-gli-hacker-filo-russi-hanno-sferrato-al-csm/)

I RISCHI DELLA CYBERSECURITY PER IL 2023

10 marzo – La guerra in Ucraina e la conseguente instabilità sociopolitica ed economica ha spostato gli equilibri mondiali di ogni settore. Anche **la cybersecurity ha risentito molto degli scossoni causati dagli ultimi eventi**, e ora è costretta ad affrontare un panorama di minacce informatiche mutevole e sempre più aggressivo.
Il ***Cyber Working Group*** del Bipartisan Policy Center di Washington ***ha analizzato i principali rischi per la cybersicurezza per il 2023***, identificando quelli considerati più imminenti da risolvere e dagli impatti potenziali più disastrosi.
(source: https://www.securityinfo.it/2023/03/10/rischi-cybersecurity-2023/)

CYBERSECURITY, FATTORE UMANO COME PRIMA LINEA DI DIFESA

10 marzo – *Investire in formazione per rispondere all'impennata di attacchi cyber e proteggere il valore aziendale. Mercato della sicurezza in crescita, ma in Italia mancano i professionisti. La sfida delle competenze e la necessità di una cultura organizzativa resiliente.*
La formazione rappresenta una delle risposte più efficaci che le aziende possono mettere in atto per rispondere all'impennata di attacchi cyber. Serve una solida e diffusa cultura della sicurezza informatica in grado di incidere sulle capacità organizzative e ridurre i rischi. La carenza di competenze in ambito security affligge da diversi anni le aziende di tutti i settori.
(source: https://www.datamanager.it/2023/03/cybersecurity-fattore-umano-come-prima-linea-di-difesa/)

CYBERCRIME, I TRASPORTI ITALIANI NEL MIRINO DEGLI HACKER RUSSI

24 marzo – Attaccati i siti del Ministero, dell'Autorità di regolazione e dell'Atac. L'offensiva è di tipo Ddos per mettere fuori uso accesso e operatività dei servizi. A Roma biglietterie in tilt. Appena qualche giorno fa presi di mira i portali della Difesa e del Consiglio superiore della magistratura.
(source: https://www.corrierecomunicazioni.it/cyber-security/cybercrime-i-trasporti-italiani-nel-mirino-degli-hacker-russi/)

LA POTENZA DI GPT-4: L'AI DI MICROSOFT STA PER SORPRENDERCI CON UN SUPER COMPUTER DI ULTIMA GENERAZIONE!

23 marzo – *OpenAI*, che ha avuto molto successo con ChatGPT, sta continuando ad esplorare i modelli di linguaggio di grandi dimensioni e ha lanciato una nuova generazione di modelli di elaborazione del linguaggio naturale, *GPT-4*.
Secondo quanto riportato sul sito ufficiale di OpenAI, il nuovo GPT-4 è il sistema più avanzato finora mai realizzato.
Ha capacità di risoluzione dei problemi più accurate ed è superiore a *ChatGPT*, che è stato lanciato nel novembre dello scorso anno e ha oltre 100 milioni di utenti.
(source: https://www.redhot-cyber.com/post/la-potenza-di-gpt-4-lai-di-microsoft-sta-per-sorprenderci-con-un-super-computer-di-ultima-generazione/)

CYBERSECURITY, IN ITALIA PROFESSIONISTI "SOTTOPAGATI"

22 marzo – egli ultimi anni la minaccia di incidenti informatici si è estesa a tutte le tipologie di aziende, non solo grandi operatori, ma anche imprese di piccola e media dimensione che hanno sistemi di difesa più penetrabili e possono anche rappresentare un veicolo per insinuarsi tra le maglie di difesa di organizzazione di dimensioni più grandi.
Per rinforzare le strutture di cyberdifesa in Italia, uno degli aspetti chiave è quello della formazione delle competenze, dell'attrazione dei talenti, della capacità di trattenere risorse esperte e qualificate. Risorse che però sono scarse. Stando alle stime di Acn, l'Agenzia per la cybersicurezza nazionale, ci sarebbe una carenza di 100mila esperti in cybersecurity per coprire le esigenze di imprese e PA. A questo si aggiunge il fatto che i livelli retributivi degli specialisti nel settore sono nettamente più bassi nel nostro Paese, soprattutto se confrontati con le realtà degli Usa e del Regno Unito. **In *un paper* il Centro Studi Tim evidenzia le maggiori criticità.**
(source: https://www.corrierecomunicazioni.it/digital-economy/cybersecurity-in-italia-professionisti-sottopagaticybesecurity-in-italia-professionisti-sottopagati/)

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 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

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:

GET CERTIFIED

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.