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

Newsletter

ANNO 2022 | N. 10 | NOVEMBRE

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 WEAPONIZZAZIONE DEL SOFTWARE E I TENTATIVI NORMATIVI DI PREVENZIONE

Anche se non esiste una definizione ufficiale di Cyberweapon, alcune pubblicazioni ne hanno definito le caratteristiche: "un oggetto progettato e sviluppato o ottenuto per lo scopo principale di uccidere, mutilare, ferire, danneggiare o distruggere" (Legal Reviews of Cyber Weapons' (2014), "mezzi di guerra informatici utilizzati, progettati o destinati a essere utilizzati per causare lesioni o morte di persone o danni o distruzione di oggetti" (Tallinn Manual 2.0); "qualsiasi dispositivo, programma per computer o script per computer, inclusa qualsiasi combinazione di software, firmware o hardware destinati a negare, interrompere, degradare, distruggere o manipolare informazioni, sistemi informativi o reti di obiettivi avversari" (Air Force Instruction 51-401 (2018).

Qualunque sarà la definizione ufficiale secondo il Centro di difesa informatica cooperativa della NATO di Tallin (CCDCOE) tutti gli strumenti informatici in grado di condurre "attacchi" come intesi nel Diritto Internazionale Umanitario (IHL), cioè atti di violenza contro l'avversario sia in offesa che in difesa, dovrebbero essere considerate come armi informatiche, rientrando quindi nel principio secondo cui l'IHL si applica a "tutte le forme di guerra e a tutti i tipi di armi, quelle del passato, quelle del presente e quelle del futuro". Quindi un malware impiegato per obiettivi militari, paramilitari o di intelligence è un'arma informatica. Sample di malware universalmente riconosciute come Cyberweapon sono ad esempio: Duqu, Flame (malware), Great Cannon, Mirai (malware), Wiper (malware), Pegasus (spyware) e naturalmente Stuxnet nota come la prima di questa serie e l'ultima in ordine cronologico Acidrain apparsa durante il conflitto Russo Ucraino.

Stuxnet è stato un potente worm informatico progettato dall'intelligence statunitense e israeliana per disattivare una parte fondamentale del programma nucleare iraniano; identificato per la prima volta dalla comunità infosec nel 2010, lo sviluppo su di esso è iniziato probabilmente nel 2005.

AcidRain, invece, stato un attacco mirato contro un server Viasat in Italia che gestiva un gran numero di modem, e quindi di comunicazioni internet, in tutta Europa e in Ucraina. L'attacco è stato programmato prima dell'invasione dell'Ucraina da parte della Russia per degradarne le comunicazioni ed ottenere un vantaggio tattico sul campo di battaglia.

È importante chiarire che con il termine "armare il software" la comunità Infosec non indica solo le Cyberweapon sopraccitate, ma anche la pratica di iniettare software malevolo in un codice originariamente innocuo per compiere azioni criminali anche solo per Cybercrime. In particolare, il Microsoft Threat Intelligence Center (MSTIC) ad ottobre ha rilevato un'ampia gamma di tentativi di phishing che utilizzano software open source appositamente "armati" da un gruppo di attacco noto come ZINC/Lazarus Group che dopo una prima fase di ingegneria sociale divulgava payload a mezzo WhatsApp, ovvero versioni malevole di software open source leciti tra cui PuTTY, KiTTY (entrambe client di

servizi SSH/telnet) e il programma di installazione *TightVNC* (un software di free remote desktop), in diversi settori tra cui media, difesa e aerospaziale e servizi IT in Stati Uniti, Regno Unito, India e Russia.
Dati i rischi significativi che un codice lecito e "benevolo" possa essere trasformato in un'arma cibernetica, alcune delle aziende leader a livello mondiale dedicate all'introduzione nella società di nuove generazioni di robotica mobile avanzata hanno voluto sottoscrivere una lettera aperta indirizzata all'industria robotica e alla comunità in cui hanno voluto ribadire il loro impegno a: "*non utilizzare come armi i nostri robot generici per la mobilità avanzata o il software che sviluppiamo che consente la robotica avanzata e non supporteremo altri a farlo. Quando possibile, esamineremo attentamente le applicazioni previste dai nostri clienti per evitare potenziali armi. Ci impegniamo inoltre a esplorare lo sviluppo di caratteristiche tecnologiche che potrebbero mitigare o ridurre questi rischi. Per essere chiari, non stiamo contestando le tecnologie esistenti che le nazioni e le loro agenzie governative utilizzano per difendersi e sostenere le proprie leggi. Comprendiamo che il nostro impegno da solo non è sufficiente per affrontare pienamente questi rischi, e pertanto invitiamo i responsabili politici a collaborare con noi per promuovere l'uso sicuro di questi robot e per proibirne l'uso improprio. Chiediamo inoltre a ogni organizzazione, sviluppatore, ricercatore e utente nella comunità della robotica di impegnarsi in modo simile a non costruire, autorizzare, supportare o consentire il collegamento di armi a tali robot…..*".
Il rischio è concreto dato che anche L'Interpol è preoccupata per la potenziale disponibilità di armi informatiche militari di livello militare sul dark web. Il segretario dell'Interpol Jurgen Stock ha confermato tale preoccupazione dichiarando che qualsiasi arma che vengono utilizzate sul campo di battaglia potrà un domani essere usata da gruppi della criminalità organizzata. Naturalmente non si parla solo delle armi cinetiche ma anche di quelle Cyber. I rapporti indicano che il mercato delle armi informatiche militari sta crescendo a un CAGR elevato (Compounded Average Growth Rate, rappresenta la crescita percentuale media di una grandezza in un lasso di tempo n.d.r.) per il periodo di previsione 2022-2029. (Fonte Cybertalk).
Se ci si chiede quali possano essere strumenti internazionali per evitare la diffusione di tecnologie dual use a paesi che potrebbero abusarne si ricorda che esiste il Wassenar arrangement, un accordo tra 41 paesi per disciplinare l'esportazione di tecnologie a duplice uso, al fine di scoraggiare le vendite a regimi totalitari. Molte tecnologie hanno avuto nella storia un duplice uso tanto nel bene quanto nel male. Un esempio è la fissione nucleare…ma anche gli strumenti digitali possono essere benevoli o malevoli secondo il loro utilizzatore: rappresentano strumenti per individuare falle nelle difese di rete oppure gli stessi codici di intrusione possono costituire armi d'assalto digitali, consentendo alle persone di ascoltare le conversazioni di altre persone e rubare i loro dati. Per questo motivo nel 2013 l'Accordo di Wassenar è stato aggiornato per includere le tecnologie di sorveglianza basate su Internet, utilizzabili in quei paesi dove alcuni diritti umani non sono garantiti. Tuttavia, l'accordo di Wassenar non è un trattato vincolante, quindi i paesi implementano questi controlli a loro proprio modo. Nonostante la pubblicazione da parte degli Stati Uniti di una *proposta specifica in materia di export di prodotti di Cybersecurity*, l'industria della sicurezza informatica non l'ha appoggiata ritenendola troppo ampia discrezionale e arbitraria in termini di implementazione. Piuttosto è stata creato la *Coalition for Responsible Cybersecurity* per respingere le regole proposte e per esortare: "*le nazioni membri di Wassenaar a restringere e concentrare i controlli sul "software di intrusione", compresa la revisione della definizione eccessiva di "software di intrusione" e la limitazione dei controlli su software, hardware, tecnologia e condivisione di informazioni critici per la sicurezza informatica..*" Parimenti la coalizione si è dichiarata preoccupata per le possibili restrizioni alla ricerca applicata nella cybersecurity fra paesi diversi, per le conseguenze negative del mancato sviluppo ed evoluzione delle tecnologie e per i controlli preventivi prima di vendere alcune tecnologie Cyber fuori dal confine americano. Per la coalizione quindi, le restrizioni sono sembrate troppo stringenti e darebbero al governo americano un poter discrezionale e arbitrario lesivo delle regole di libera concorrenza.
L'ultima fase è rappresentata dalla pubblicazione di una *norma definitiva il 21 ottobre 2021* dal Bureau of Industry & Security (BIS) del Dipartimento del commercio degli Stati Uniti che ha modificato le Export Administration Regulations (EAR) e ha creato nuove licenze e requisiti per l'esportazione o il trasferimento di articoli di sicurezza informatica verso paesi non statunitensi. Si concentra su hardware, software e tecnologia (collettivamente indicati nell'EAR come "articoli") con funzionalità di sicurezza informatica. La norma vorrebbe limitare le attività informatiche dannose, soprattutto per evitare il controllo globale mediante strumenti digitali, ma ha implicazioni significative e aggiunge una notevole complessità alla più ampia comunità della sicurezza informatica anche se sono state previste delle eccezioni

per garantire commercio e sviluppo. La proposta è divenuta esecutiva da gennaio 2022.
Naturalmente il conflitto Russo Ucraino ha dato un nuovo impulso all'uso malevolo delle tecnologie digitali e costretto tutti i paesi ad una reale e ulteriore riflessione. Thomas Rid, esperto mondiale di cyber sicurezza sostiene che: "*La guerra cibernetica non è mai avvenuta in passato, non si verifica nel presente ed è altamente improbabile che possa disturbare il nostro futuro*", ma molti professionisti ritengono che una Cyber War come fenomeno autonomo sia improbabile e che piuttosto le cyberweapon sembrano essere usate come uno strumento aggiuntivo, ma non sostitutivo dei convenzionali atti di forza.

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 02 DICEMBRE 2022

ORE 15:00-18:30

"SICUREZZA, PRIVACY E INTELLIGENZA ARTIFICIALE"

Algoritmi, intelligenza artificiale, machine learning, trust ed etica: è stato scritto molto sull'argomento, ma quali sono i "fondamentali" da cui partire per affrontare i vari aspetti della relazione tra Sicurezza, Privacy ed Intelligenza Artificiale?
Una volta definita la prospettiva di osservazione, saranno discussi elementi normativi emergenti a livello europeo, identificati impatti del GDPR, e sarà presentata un'ipotesi di ambito di valutazione del rischio – in particolare rispetto alle valutazioni ethics-based. Infine, vedremo come si stanno evolvendo framework e standard per adeguarsi all'era dell'algoritmo.

*Relatrice**: Dott.ssa Francesca Della Mea***
Laureata in Economia Aziendale e Organizzazione presso l'Università Bocconi di Milano, ha maturato un'esperienza di oltre 20 anni in ambito Information Security, prima in Microsoft, poi in Accenture dove ha sviluppato e gestito la practice Accenture Security per l'area IGEM. Successivamente è stata responsabile di practice di consulenza security in aziende specialistiche, gestendo programmi di trasformazione digitale per clienti enterprise (5000-10000 dipendenti). Interessata in particolare a nuovi modelli gestionali per ICT e security, allineamento business-ICT, business security architecture, information risk management, ICT compliance, Security Operations, Security Analytics.
Fa parte del Gruppo di lavoro ISACA Roma su FAIR, dedicato all'analisi quantitative del rischio. È certificata CISM, CISA, CCSK, LBBP (Sigma Lean Black Belt Professional). Ha studiato cinese (HSK4) e si tiene aggiornata sullo scenario asiatico

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

LE PRINCIPALI NOTIZIE

AGENZIA PER LA CYBERSICUREZZA NAZIONALE, ACCORDO CON ACCREDIA PER CYBERSECURITY

28 novembre 2022 – (Adnkronos) - La certificazione accreditata è uno dei principali strumenti a disposizione di imprese e istituzioni per garantire un'adeguata sicurezza informatica di prodotti e servizi digitali: più aumentano gli enti dotati di certificazione accreditata per la sicurezza delle informazioni più diminuisce il rischio di esposizione agli attacchi informatici. Il Decreto Legislativo n.123 del 3 agosto 2022, che recepisce il Titolo III del Regolamento UE n. 881/2019, ha previsto che alcune tipologie di certificazioni in ambito cybersicurezza potranno essere rilasciate da Organismi di valutazione della conformità accreditati da Accredia, che lavorerà insieme all'Agenzia per la Cybersicurezza Nazionale nel monitoraggio e nella vigilanza delle attività di tali organismi.

(source: https://it.notizie.yahoo.com/agenzia-per-la-cybersicurezza-nazionale-211100402.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAC4wVq7cJ8kriJY22UN-MNgBFblD3EF49Q2ccZc62Br6A4DFHg06SQQ4AWw5kSxnodYe3PtlawYBKfIZWEzIV4jfzKgCClTSmeFIRgXFr-5ECzemkdWHn0ptKWadlsDxD-LUMe8GuEC9PLcWMqWF3CB_LbS5jwtSftQUNb5gQhvNHQ)

FBI LANCIA L'ALLARME: TIKTOK È UN PROBLEMA DI SICUREZZA NAZIONALE

03 dicembre 2022 – **TikTok è un problema di sicurezza nazionale**. A lanciare l'allarme è il direttore dell'Fbi, Chris Wray, rilevando che l'app per la condivisione di video, popolarissima tra i più giovani, è nelle mani del governo cinese, "che non condivide i nostri valori".

(source: https://www.rainews.it/articoli/2022/12/fbi-lancia-lallarme-tiktok--un-problema-di-sicurezza-nazionale-28c94543-aeec-4d3a-bb2d-2e7acb656eff.html)

CYBERSECURITY, I TRE CASI ANALIZZATI DALL'AGENZIA NAZIONALE: ECCO COME DIFENDERSI DALLE TRUFFE

29 novembre 2022 – na pagina hackerata, una consegna non effettuata, un'allettante abboccamento per eventuali proposte di lavoro: sono tre distinte situazioni in cui chi legge potrebbe essersi imbattuto in passato. Magari, per aver ricevuto - sul proprio cellulare o via posta elettronica - una comunicazione che ai più "navigati" frequentatori del web sarà risultata quantomeno "sospetta". Ma che, a quanti masticano poco di e-mail, spam e altre comunicazioni virtuali (in realtà, ormai pochi), poteva risultare perfettamente normale come le altre (tante) a cui si risponde ogni giorno.

(source: https://www.rainews.it/articoli/2022/11/cybersecurity-agenzia-nazionale-come-difendersi-truffe-faeaae11-d2cf-48a0-b8f3-5e32ec315204.html)

BALDONI (ACN): 'INTELLIGENZA ARTIFICIALE LEGATA A TRASFORMAZIONE DIGITALE'

01 dicembre 2022 – (Adnkronos) - "Il tema dell'intelligenza artificiale è intrinsecamente legato alla velocità della trasformazione digitale: più si affermerà e più la trasformazione digitale aumenterà il suo impatto. Come la cybersecurity, l'intelligenza artificiale è un tema olistico. Non abbiamo solo bisogno di tecnici preparati sul tema, ma anche di tutta una serie di figure con varietà di competenze e background, che ci aiutino a navigare nella complessità del mondo sempre più tecnologico". Ad affermarlo è stato Roberto Baldoni, Direttore Generale, Agenzia per la Cybersicurezza Nazionale, intervento alla presentazione a Roma della ricerca 'Intelligenza Artificiale: una sfida contemporanea' realizzata dall'International Corporate Communication Hub con la Iulm.

(source: https://it.finance.yahoo.com/notizie/baldoni-acn-intelligenza-artificiale-legata-183841650.html)

CYBERSECURITY: IL VADEMECUM DEL GARANTE PER PASSWORD A PROVA DI PRIVACY

27 novembre 2022 – Password, PIN, metodi di autenticazione a due fattori, dati biometrici: sono tante le modalità attraverso le quali i sistemi informatici cercano di garantire la sicurezza nell'accesso a profili e servizi personalizzati. Ma soprattutto per quelli più delicati, come ad esempio le piattaforme di pagamento e le attività finanziarie, ma anche i server aziendali, i pericoli di violazione dei sistemi sono sempre in agguato e ciò vale in particolare per le password, i codici alfanumerici scelti dagli utenti in maniera non sempre "inespugnabile". Secondo recenti studi, sono particolarmente diffuse password facilmente identificabili, come ad esempio 123456.

(source: https://gazzettadelsud.it/articoli/noi-magazine/2022/11/27/cybersecurity-il-vademecum-del-garante-per-password-a-prova-di-privacy-b69854f8-7a60-4ef3-9caf-d2081e6c2e01/)

UNIVERSITA' ITALIANE NEL MONDO - DOTTORATO DI RICERCA IN CYBERSECURITY : COLLABORAZIONE LA SAPIENZA (ROMA) /LUISS GUIDO CARLI

28 novembre 2022 – Nell'Aula magna del Dipartimento di Informatica e sistemistica Antonio Ruberti della Sapienza, è stato inaugurato il Dottorato di ricerca in Cybersecurity, promosso da Sapienza in collaborazione con l'Università Luiss Guido Carli.

All'inaugurazione sono intervenuti la rettrice della Sapienza Antonella Polimeni, il rettore della Luiss Guido Carli Andrea Prencipe, il vice presidente Università Luiss Guido Carli Paola Severino, la direttrice del Dipartimento di Ingegneria informatica automatica e gestionale Tiziana Catarci, il coordinatore Dottorato di ricerca in Cybersecurity Leonardo Querzoni.

(source: https://www.italiannetwork.it/news.aspx?ln=it&id=73111)

CERTIFICAZIONE ISO 27001 – 27017 – 27018: LA SICUREZZA DELLE INFORMAZIONI INDUSTRIALI, COMMERCIALI E AZIENDALI SECONDO LA ICP SRL

25 novembre 2022 – (Adnkronos) – Roma, 25 novembre 2022. Con l'evoluzione del mercato e l'intensificarsi dei fenomeni di "cyber crime" è ormai di fondamentale importanza avere piena padronanza e controllo sui fattori della "Terna R.I.D." (Riservatezza, Integrità e Disponibilità). Avere il massimo controllo su questi tre parametri fa infatti oggi la differenza tra un'azienda pronta a cavalcare il "rischio del successo" e un'azienda che si troverà quasi certamente travolta da onde anomale impetuose.
(source: https://www.italiaambiente.it/2022/11/25/certificazione-iso-27001-27017-27018-la-sicurezza-delle-informazioni-industriali-commerciali-e-aziendali-secondo-la-icp-srl/)

INTELLIGENZA ARTIFICIALE E CYBER SECURITY: SERVONO COMPETENZE PER LA DIFESA DELLE INFRASTRUTTURE CRITICHE

05 dicembre 2022 – È necessaria una **maggiore cooperazione tra settore pubblico e privato** al fine di **facilitare le soluzioni e lo sviluppo di competenze e tecnologie per il settore delle infrastrutture critiche** e per **affrontare le sfide poste dal cyber spazio**.

Di questo si è parlato nelle giornate del 21 e del 23 novembre 2022 durante le quali si è tenuta la **quarta edizione del Canada-Italy Business Forum** su **intelligenza artificiale (AI) e cyber sicurezza**: un ciclo di incontri che ha radunato enti governativi canadesi e italiani, imprese tecnologiche, università, PMI e startup, oltre che relatori esperti.
Visto l'attuale panorama in tema di cyber security, la sessione più rilevante è sicuramente stata quella dedicata alla "*Critical Infrastructures, Defense and Space*".
(source: https://vincos.it/2022/10/29/intelligenza-artificiale-generativa-le-applicazioni/)

ATTACCHI HACKER, L'ALLERTA DELL'AGENZIA PER LA CYBERSICUREZZA: "RISCHIO ATTI DIMOSTRATIVI CONTRO SITI ISTITUZIONALI ITALIANI"

05 dicembre 2022 – Attacchi **dimostrativi** potrebbero colpire i siti istituzionali italiani. È l'allerta lanciata dal **Csirt,** il team di risposta in caso di incidenti **dell'Agenzia per la cybersicurezza nazionale**. Non risulta comunque, precisa **l'Agenzia**, che gli attacchi – a quanto appare attualmente di carattere "dimostrativo" – abbiano intaccato l'integrità e la confidenzialità delle informazioni e dei sistemi interessati. Si raccomanda dunque di "mantenere alto il livello di attenzione sulla protezione delle proprie infrastrutture informatiche, di verificare e aumentare le misure di protezione relative agli attacchi DDoS. Attacchi che, secondo alcune fonti aperte, sono destinati a continuare o intensificarsi nei prossimi mesi". L'origine degli attacchi? Secondo fonti aperte arriverebbero da gruppi **hacktivisti**, di origini russe.
(source: https://www.ilfattoquotidiano.it/2022/12/05/attacchi-hacker-lallerta-dellagenzia-per-la-cybersicurezza-rischio-atti-dimostrativi-contro-siti-istituzionali-italiani/6895909/)

CYBERSECURITY, IL PROBLEMA STA NEL MANICO E CISCO LO EVIDENZIA

05 dicembre 2022 – Il 99% delle aziende si trova al di sotto della "linea di povertà" nella **cybersecurity**. Il concetto è stato coniato, già da diversi anni, da **Wendy Nather**, responsabile della consulenza per i Ciso in **Cisco**. L'esperta identifica con questa definizione una sorta di invisibile divisorio fra coloro che sanno come implementare le corrette misure di protezione e quelli che non ne sono capaci.
Quello della "**cybersecurity poverty line**" è un concetto diffusosi fra gli analisti, tanto che **Gartner** da un paio d'anni parla di "cyber 1%" per identificare la piccolissima parte di imprese che possiedono risorse, cultura e struttura adatte una postura di eccellenza nella difesa dalle minacce.
(source: https://www.ictbusiness.it/cont/news/cybersecurity-il-problema-sta-nel-manico-e-cisco-lo-evidenzia/47249/1.html#.Y45oTOzMIQ)

NUOVA ISO 27001:2022: COSA CAMBIA, I PUNTI DI ACCORDO COL GDPR E COME ADEGUARSI

11 novembre 2022 – Lo scorso mese di ottobre è stata *pubblicata* la **ISO 27001:2022**, lo standard che specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un ***sistema di gestione della sicurezza delle informazioni (ISMS)***.
Prima di scoprirne le novità e capire cosa succederà adesso per le aziende che dovranno adeguarsi, iniziamo subito con le buone notizie: se già abbiamo un sistema certificato, fino a ottobre 2023 gli audit potranno essere condotti in base alla versione 2013 o, su nostra richiesta, alla ISO/IEC 27001:2022.
(source: https://www.cybersecurity360.it/legal/nuova-iso-270012022-cosa-cambia-i-punti-di-accordo-col-gdpr-e-come-adeguarsi/)

CITAZIONI IN TRIBUNALE? ATTENTI ALLA TRUFFA: I DETTAGLI DEL MESSAGGIO

11 novembre 2022 – Il mondo criminale con l'avanzamento della rete si è sempre più adeguato. I **truffatori** non hanno perso tempo ed ha messo in campo delle tecniche per rubare soldi e informazioni delle potenziali vittime. La particolarità è che riescono a "travestirsi" anche da importanti autorità ma non sempre i dettagli sono corretti
(source: https://www.chenews.it/2022/11/11/citazione-tribunale-truffa/)

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/*