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

Newsletter

ANNO 2022 | N. 05 | MAGGIO

ISACA (Information Systems Audit and Control Association)

L'ISACA, (Information Systems Audit and Control Association), ha 144.112 associati in oltre 188 nazioni (dato aggiornato a luglio 2020) 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

SECURITY AUDITING PER AGLI AMBIENTI CLOUD: COME È POSSIBILE OPERARE E SU QUALI FATTORI

Entro il 2025 ci saranno circa 100 zettabyte di dati (ovvero 100 miliardi di GB) archiviati nel cloud a livello globale (fonte: *The 2020 Data Attack Surface Report*), una straordinaria superficie potenziale di attacco che necessita di audit di security per una verifica del suo livello di protezione.

Per chi ha già dimestichezza con lo svolgimento di un audit è noto che sia il processo di esame e revisione sistematica di dati, informazioni, asset, registrazioni e documenti di un'entità in modo da verificarne l'accuratezza, l'affidabilità, la legittimità e la completezza. L'obiettivo di un audit cloud è controllare e migliorare la disponibilità dei dati ed esaminare l'affidabilità dei controlli di sicurezza, che dovrebbero essere assicurati dal fornitore di servizi cloud. Il processo di solito prevede un'indagine tecnica e la presentazione dei risultati sotto forma di un rapporto che, dipendentemente dal tipo di audit, può riportare informazioni sull'efficienza delle prestazioni dell'infrastruttura cloud esistente, valutazione dei costi e sui mezzi di controllo in ambito sicurezza. Infatti, i tipi di audit nel cloud computing possono essere distinti fra:

- Audit dell'infrastruttura cloud, della sicurezza, delle prestazioni e della valutazione dei costi: in questo caso si rilevano configurazioni errate, vulnerabilità e minacce dell'infrastruttura all'interno dell'ambiente cloud. Si verifica anche che la capacità di registrazione e monitoraggio siano sufficienti e si esaminano le politiche di accesso e sicurezza, il livello di crittografia delle informazioni e se i dati archiviati nel cloud sono protetti sia "in transit" che "at rest".
- Audit delle vulnerabilità: valutazione dei punti deboli della sicurezza che rappresentano una minaccia per l'affidabilità e la sicurezza del sistema informatico. Solitamente si utilizzano scanner automatizzati per verificare i limiti della rete interna ed esterna, i sistemi e le applicazioni Web per le vulnerabilità note. Gli audit di scansione delle vulnerabilità forniscono un riepilogo completo di ogni potenziale punto di attacco e debolezza riscontrato.
- Verifica e hardening della configurazione: il processo di verifica che i sistemi siano protetti preventivamente e proattivamente dagli attacchi. Il controllo garantisce che la configurazione di sicurezza di un sistema sia impostata in modo appropriato, che il software del sistema operativo venga aggiornato per stare al passo con i nuovi exploit e che questo processo venga eseguito continuamente, utilizzando la massima automazione possibile.

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

- Hardening della configurazione della pipeline SDLC (Software Development Life Cycle) e audit di revisione: controllare la configurazione dell'ambiente SDLC è cruciale poiché questo processo è alla base della creazione di software funzionante. Se la pipeline CI/CD (pratiche combinate di Integrazione Continua e Consegna Continua o Distribuzione Continua, *NdR*) non è sicura, i dati sensibili potrebbero essere esposti a fonti esterne.

Le *checklist* per l'analisi e il controllo della conformità per gli ambienti cloud rappresentano un modo semplice per iniziare e assicurare che tutte le attività di cloud computing siano rispettose rispetto alla compliance verso la regolamentazione e verso le autority che chiedono trasparenza sulla proprietà e sull'accesso ai dati. Ma la compliance non è tutto. Negli ultimi anni gli ambienti cloud sono stati oggetto e soggetto di attacchi generalizzati e progressivamente sempre più sofisticati che hanno dimostrato quanto l'attenzione alla sicurezza informatica sia fondamentale e come sia necessario renderla un elemento contrattuale con il provider per tutelare la propria organizzazione. Infatti, i sistemi di cloud computing introducono una serie di rischi e sfide che non sono presenti allo stesso modo negli ambienti on premise. Le sfide comprendono quattro elementi basilari:

- Il fornitore di servizi ha il controllo completo dell'infrastruttura.
- I dati vengono archiviati su un numero di server in più posizioni fisiche.
- L'accesso ai servizi da parte di soggetti esterni può essere controllato direttamente o tramite altri servizi forniti dal fornitore.
- È possibile accedere ai servizi cloud da qualsiasi parte del mondo, in qualsiasi momento e in qualsiasi momento.

Per un cloud provider le criticità di sicurezza riguardano: vulnerabilità di sicurezza del codice o dei sistemi operativi, utenti malintenzionati che accedono alle informazioni tramite una backdoor o un altro percorso precedentemente sconosciuto, accesso mediante identità utente violata a mezzo phishing o brute force attack, accesso non autorizzato mediante accesso fisico a informazioni sensibili (backup di un cliente), minacce interne perpetrate da insider che danneggia deliberatamente i beni dell'azienda accedendovi in modo inappropriato.

La *Checklist per l'assesment della sicurezza in Cloud* mira a fornire un elenco ad alto livello delle aree di sicurezza da considerare nell' ambiente cloud. Le aree di analisi riguardano:

- Identificazione dei punti deboli e dei potenziali punti di ingresso nell'infrastruttura cloud dell'organizzazione.
- Analisi della rete per tentare di sfruttarne le falle.
- Identificazione di approcci di sicurezza per prevenire attacchi futuri.

Più in dettaglio è necessario analizzare le aree di:

- Postura generale di sicurezza: mediante interviste ed esame documentale si valuta la postura di sicurezza dell'infrastruttura cloud aziendale.
- Controllo e gestione degli accessi: si esaminano i processi di gestione delle identità e degli accessi, inclusi gli account utente, i ruoli e la gestione delle chiavi di accesso.
- Sicurezza della rete: la segmentazione della rete e le politiche del firewall sono esaminate per errori di configurazione comuni.
- Gestione degli incidenti: si esamina la politica di risposta agli incidenti relativa all'infrastruttura cloud, inclusi ruoli e processi relativi a un incidente.
- Sicurezza dell'archiviazione: si valuta lo stato dell'archiviazione cloud, inclusi l'archiviazione a livello di oggetto, l'archiviazione a livello di blocco e gli snapshot associati.
- Sicurezza dei servizi di piattaforma: si valuta e analizza la configurazione di sicurezza delle offerte di servizi avanzati specifiche per ciascun provider di servizi cloud.
- Sicurezza del carico di lavoro: la sicurezza è esaminata in relazione ai carichi di lavoro, inclusi i server virtualizzati, i container ospitati dal server, le funzioni e i carichi di lavoro containerizzati senza server.

In generale gli audit controllano l'implementazione delle best practices per la sicurezza del Cloud, la loro impostazione e implementazione nonché il test periodico. Un *elenco esaustivo di tali buone prassi può essere consultato sul sito della guida PCIDSS*.

È bene infine ricordare che sia il fornitore di servizi cloud che il cliente hanno la responsabilità di mantenere un sistema sicuro secondo il *modello di responsabilità condivisa (Shared Responsibility Model –*

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

Cloud Security Alliance – CSA). L'attuazione e il monitoraggio di politiche e procedure complete contribuiranno a migliorare quest'area che comunque costituisce un ulteriore settore di rischio.
Quale che sia il modello di Cloud prescelto in funzione anche del modello di responsabilità, è buona regola tutelarsi mediante l'introduzione di alcune clausole nel contratto con il Cloud Provider. La European Banking Association – EBA è intervenuta sull'argomento cloud computing nel 2017 con proprie "*Raccomandazioni in materia di esternalizzazione a fornitori di servizi cloud*". Nelle proprie Raccomandazioni l'EBA individua i seguenti elementi di attenzione e valutazione

- Valutazione della rilevanza dell'attività esternalizzata
- Obbligo di informare le autorità di vigilanza o controllo
- Diritti di accesso e audit
- Sicurezza dei dati e dei sistemi
- Localizzazione dei dati e trattamento dei dati
- Esternalizzazione «a catena»
- Piani di emergenza e strategie di uscita.

In Italia è il *Vademecum predisposto dal Garante per la protezione dei dati personali* che suggerisce alcune "Raccomandazioni" agli utilizzatori prima di considerare il ricorso ad un servizio di cloud computing:

- Effettuare una verifica sull'affidabilità del fornitore
- Privilegiare i servizi che favoriscono la portabilità dei dati
- Assicurarsi la disponibilità dei dati in caso di necessità
- Selezionare i dati da inserire nella "nuvola"
- "Non perdere di vista" i dati
- Informarsi su dove risiederanno, concretamente, i dati
- Attenzione alle clausole contrattuali (responsabilità, portabilità)
- Verificare tempi e modalità di conservazione dei dati
- Esigere adeguate misure di sicurezza
- Formare adeguatamente il personale

Per ogni dettaglio su ciascuna delle sopraccitate aree di accordo, preventivamente alla stipula del contratto, si consiglia di *approfondire anche usando le indicazioni dell'avvocato Luigi Neirotti*, esperto di data protection, affinché il tema della sicurezza diventi un tema cruciale per tutte le parti.

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.
L'intenzione è quella di:

- avvicinare le community nazionali di **ISIPM** e **ISACA**
- ampliare le aree di interesse delle due community
- favorire lo scambio di esperienze e conoscenze
- aumentare il grado di formazione e di competenza nelle tematiche di interesse delle due organizzazioni
- organizzare congiuntamente eventi e/o webinar di "Project Management" e ICT Security Management, per sensibilizzare i propri soci sull'importanza di tali discipline e delle relative metodologie e tecniche.

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

- sviluppare percorsi formativi congiunti, che uniscano la formazione per le certificazioni di **ISACA (CSX® fundamentals**, **CSX-P**, **CISA®**, **CISM®**, **CGEIT®** e **CRISC®)**, a quella per la certificazione **ISIPM-Base®** e alla qualificazione **ISIPM-Av®** di **ISIPM** (1° e 2° livello di certificazione PM). L'obiettivo è fornire le competenze organizzative, tecniche, ed operative in materia di **Cyber-Security,** insieme alle conoscenze di **Project Management**, utili e necessarie per coloro che partecipano a progetti in vari ruoli o intendono qualificarsi.
- sviluppare e sostenere gruppi di lavoro congiunti, per studiare e creare nuove opportunità, che possono avvicinare sempre di più le due discipline, su obbiettivi comuni.

Informiamo i Soci e i followers di ISACAROMA che, con il perdurare delle disposizioni volte a contrastare la diffusione del virus COVID-19 (Coronavirus), 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* Riprenderemo gli eventi in presenza appena sarà possibile.
Vi terremo informati, per il momento vi auguriamo buona lettura!

CSXP™
Certified Cybersecurity Practitioner

ISACA Roma ha attivato il percorso, teorico e pratico con esercitazioni, per ottenere la certificazione "CSX Practitioner Certificate". Il capitolo di Roma è uno dei pochi in Europa e nel mondo ad aver completato l'iter che consente di erogare lezioni anche on-line e di fornire agli studenti la possibilità di esercitarsi con 70 laboratori virtuali.

CSX-P è stato introdotto da ISACA nel 2015 certificazione indipendente dai fornitori e basata sulle abilità a risolvere problemi, per i professionisti dell'information security e cybersecurity. CSX-P richiede ai candidati di dimostrare le proprie capacità nella cybersecurity in un ambiente dinamico e virtuale, cimentandosi su scenari attuali di cyber security, e non semplicemente superare un esame con domande a risposta multipla.

È la sola certificazione completa basata sulle performance individuali nel settore che verifica l'abilità del candidato di svolgere compiti tecnici nelle cinque funzioni di sicurezza definite dal framework NIST – identify, protect, detect, respond and recover. Ai candidati è richiesto di mettere in pratica le competenze acquisite sulla cybersecurity e dimostrare di possedere le abilità necessarie per reagire a un ambiente di minacce cyber sempre più aggressivo e vario.

CSX Practitioner Certificate consiste nel:

1. risolvere i compiti presenti in 10 laboratori virtuali

2. superare l'esame

3. dimostrare di possedere i requisiti per la certificazione (esperienza pluriennale, possesso di ulteriori certificazioni).

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

Sono disponibili due tipologie di laboratori virtuali:

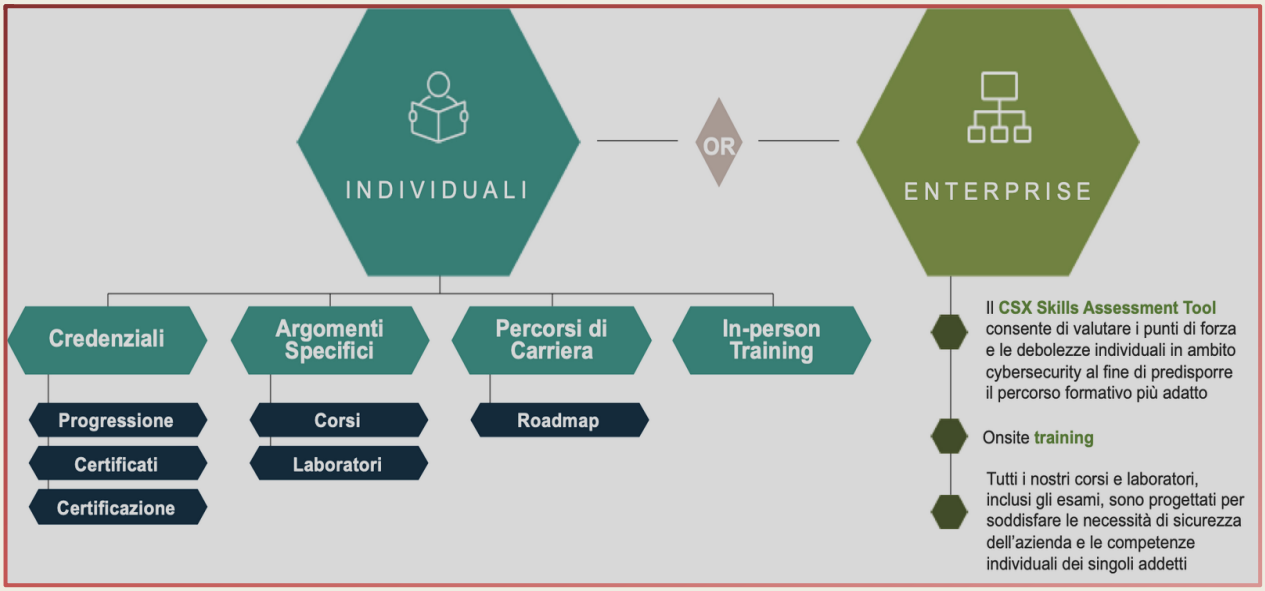
- **Laboratori on-line** – Laboratori realizzati da ISACA International e fruibili come parte integrante dei nostri corsi.
- **Laboratori specialistici esclusivi** – In aggiunta a quelli offerti da ISACA il nostro team di specialisti in ambito cybersecurity e sistemistico ha sviluppato una serie di laboratori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

È stato anche realizzato un laboratorio permanente per sessioni di Cyber Range. L'attività comprende simulazioni di rete ed esercizi di attacchi che permettono ai professionisti della sicurezza di potenziare competenze, esperienza, efficacia, comunicazione e processi.

Il partecipante svilupperà competenze pratiche sulla cybersecurity oltre a una solida base teorica, il 50% di tutti i corsi comprende degli esercizi pratici di laboratorio in un **cyber ambiente virtuale**. Nello stesso tempo si approfondiranno le tecniche per rispondere agli attacchi e recuperare dati e sistemi in caso di disastro, in particolare:

- Network evaluation
- Vulnerability analysis
- Malware & incident detection
- Incidence reporting
- Safeguard implementation.

L'offerta di corsi CSX è molto varia e modulare, ciò consente anche un approccio graduale e focalizzato su specifici ambiti (penetration e vulnerability, analisys, specialist) per consentire una formazione finalizzata qualora necessaria.



Maggiori dettagli sono disponibili qui:
http://www.isacaroma.it/wp-content/uploads/2019/11/CILLI-CSX_Training_Options_IT.pdf

ISACA Roma

- **Segreteria Corsi**
- **Tel. +39 375 599 1500**
- **cybersecurity@isacaroma.it**

www.csxp.it

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

EVENTI PASSATI

VEN 29 APRILE 2022 ORE 15:00-17:00

"Protezione dei dati personali in pratica. Conseguenze e problematiche: sanzioni, data breach, trattamento di dati nella fase di assunzione e nel rapporto di lavoro"

Il GDPR e l'adeguamento ad esso della normativa italiana (Codice privacy) sono applicati da più di tre anni ed appare di significativo interesse osservare alcune conseguenze e problematiche di tale applicazione attraverso:

- *una panoramica delle sanzioni più significative (non solo dal punto di vista dell'importo di esse) comminate dalle Autorità di controllo (DPA) europee per individuare alcune linee di tendenza interpretative, da parte di tali DPA, nella applicazione del GDPR (dott. Cesare Maria De Santis Puzzonia);*
- *un focus su una serie di data breach , realmente accaduti in Italia, che possono farci toccare con mano quali aspetti tecnici ed organizzativi aziendali possono costituire elementi di debolezza nei sistemi di gestione della protezione dei dati (dott. Cesare Maria De Santis Puzzonia)*
- *un approfondimento relativo al trattamento dei dati dei lavoratori nella fase pre-assuntiva (curricula, social) e nel corso dello svolgimento del rapporto di lavoro, con un focus sui dati sanitari e sui dati giudiziari. (avv. Paola Borghi).*

I relatori:
Dott. Cesare Maria De Santis Puzzonia.
Avv. Paola Borghi

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

PROSSIMI EVENTI

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 il loro diritti.

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

Il relatore: Giancarlo Butti

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

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

POLO STRATEGICO NAZIONALE, PRESSING DI 5STELLE E LEGA E STRETTA SUI TEMPI

19 maggio 2022 – Passano gli ordini del giorno di Liuzzi e Maccanti al decreto Taglia prezzi: relazione sulle procedure di gara entro 30 giorni dall'aggiudicazione e resoconto semestrale sullo stato di avanzamento dei lavori per il cloud di Stato. La Commissione giudicatrice si insedia sotto il faro delle Commissioni Parlamentari.
(source: https://www.corrierecomunicazioni.it/digital-economy/cloud/polo-strategico-nazionale-pressing-di-5stelle-e-lega-e-stretta-sui-tempi/)

CYBERSICUREZZA: 623 MILIONI PER IL PIANO NAZIONALE

26 maggio 2022 – L'Agenzia per la Cybersicurezza Nazionale (ACN) ha presentato il **piano per la sicurezza informatica** dell'Italia che prevede un investimento di 623 milioni di euro fino al 2026.
La cosiddetta **strategia nazionale di cybersicurezza** prevede lo sviluppo e l'attuazione di una serie di misure per garantire la **protezione delle infrastrutture** e dei sistemi informativi essenziali attraverso una collaborazione tra settori pubblico e privato.
(source: https://www.punto-informatico.it/cybersicurezza-623-milioni-piano-nazionale/)

THE FUTURE OF AUDIT IN THE WORLD OF INTERCONNECTED BUSINESS

27 maggio 2022 – The COVID-19 pandemic had changed many things; one among them is the perception of the audit process as business processes have become more interconnected and interdependent. Recently, the audit community has experienced several changes, ranging from misalignment with auditees to misunderstanding about evolving risk areas as a result of technological advancements. One area that auditors face difficulty with is the networked corporate environment. Even before an audit commences, it is critical for the auditor to adopt a holistic approach to examine the interconnected business environment's entire mechanism and activities.

(source: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/the-future-of-audit-in-the-world-of-interconnected-business)

CYBERSECURITY, INTERVISTA A PAOLO LOSSA DI CYBERARK ITALIA

07 giugno 2022 – In occasione di **CyberTech Europe a Roma**, Paolo Lossa, Country Sales Manager di **CyberArk Italia**, ci racconta gli scenari e le tendenze globali della cybersecurity.
La sicurezza informatica è finalmente stata riconosciuta come un aspetto importante da parte della maggioranza delle imprese. Si tratta di un passo importante che, però, non mette automaticamente le aziende al sicuro.
La netta accelerazione dei processi di trasformazione digitale, in parte registrata a seguito della pandemia, **ha esposto dati e asset delle imprese, che hanno dovuto abilitare nuovi meccanismi di lavoro in poco tempo**. Smart working e mobility, di per sé validi approcci operativi, rischiano di indebolire la security delle società, se non ben gestiti.
(source: https://techfromthenet.it/2022/06/07/cybersecurity-intervista-a-paolo-lossa-di-cyberark-italia/)

IN RUSSIA GOOGLE È DAVANTI A UN BIVIO

07 giugno 2022 – Alena Georgobiani si definisce una liberale russa. Georgobiani, che lavora nel settore delle pubbliche relazioni e vive a Mosca, trova più affidabili i risultati del motore di ricerca di ***Google*** rispetto a quelli del rivale locale, *Yandex*. Scarica le applicazioni sul suo telefono Android dal Play Store di Google e archivia i suoi file utilizzando il servizio di archiviazione in cloud della società. Da quando a marzo Microsoft Teams *ha lasciato* la ***Russia***, Georgobiani utilizza Google Meet per la maggior parte delle sue riunioni di lavoro. *Gmail* è il suo account di posta elettronica principale da diciassette anni.
(source: https://www.wired.it/article/russia-google-guerra-fallimento-filiale-conseguenze/)

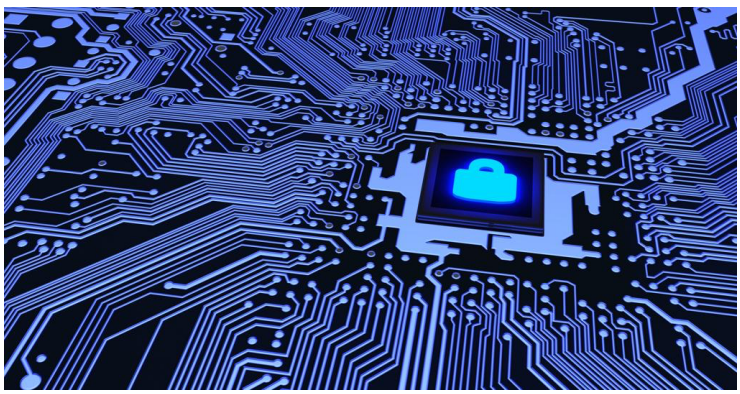
ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

I SITI CHE HANNO PUBBLICATO BUFALE SULLA PANDEMIA ORA DIFFONDONO DISINFORMAZIONE SULL'UCRAINA

06 giugno 2022 – La diffusione di notizie false è dura a morire quanto una vecchia abitudine. Secondo il centro di monitoraggio NewsGuard, un'organizzazione giornalistica che si occupa di contrasto alla disinformazione, **novantuno siti che nel 2021 avevano diffuso notizie false sulla pandemia di Covid - 19 oggi pubblicano regolarmente bufale sul conflitto in Ucraina.** Questi siti sono stati inseriti tra i più di duecento presenti nella lista del Centro di Monitoraggio della disinformazione sul conflitto Russia - Ucraina.
(source: https://www.wired.it/article/pandemia-disinformazione-ucraina/)

FURTI DI ACCOUNT WHATSAPP: ECCO COME PROTEGGERSI DALLA NUOVA CYBER TRUFFA

03 giugno 2022 – **WhatsApp** è nel mirino di una nuova cyber truffa che ruba gli account degli utenti. L'attacco è, infatti, in grado di dirottare l'app di telefonia, con tutte le chat e la rubrica, verso gli smartphone di criminali.
"Questo tipo di attacco", commenta **Paolo Dal Checco**, consulente informatico forense, "è molto più sofisticato di quello ormai noto. Infatti, i criminali negli ultimi anni convincevano le vittime a comunicare loro il codice numerico inviato via SMS". Ecco, invece, come funziona la nuova truffa e come proteggersi.
(source: https://www.cybersecurity360.it/nuove-minacce/furti-di-account-whatsapp-ecco-come-proteggersi-dalla-nuova-cyber-truffa/)



I RANSOMWARE COLPISCONO QUASI SETTE AZIENDE SU DIECI: QUINTUPLICATO IL RISCATTO MEDIO

31 maggio 2022 – Sette aziende su dieci sono nel mirino dei ***ransomware***: inoltre, è **quintuplicato** rispetto allo scorso anno il **riscatto medio** pagato per recuperare i dati. È quanto emerge dallo ***State of Ransomware 2022*** di Sophos, lo studio che analizza uno dei fenomeni più aggressivi e dannosi nell'ambito della cyber security.
"I dati che emergono dal rapporto pubblicato da Sophos sono sconcertanti", commenta **Pierluigi Paganini**, analista di cyber security e CEO Cybhorus, "anche se non sorprendono gli addetti ai lavori".
(source: https://www.cybersecurity360.it/news/i-ransomware-colpiscono-quasi-sette-aziende-su-dieci-quintuplicato-il-riscatto-medio/)

CERTIFICAZIONI DI CYBER SECURITY: IL FUTURO NEL DECRETO IN ARRIVO

09 maggio 2022 – Agenzia per la Cybersicurezza Nazionale si sta muovendo sul fronte delle **certificazioni di cyber security di prodotto**, unico punto ancora rimasto inattuato del programma dell'ACN.
Il decreto legislativo in discussione individua gli adeguamenti nazionali al quadro europeo di certificazione della cyber security: designa l'autorità nazionale di certificazione della cyber security nell'ACN, con organizzazione e procedure.
(source: https://www.telefonino.net/notizie/cybersicurezza-in-7-giorni-italia-subito-35-campagne-malevole/)

IL CLOUD COMPUTING ELEMENTO CHIAVE DELLA TECNOLOGIA 5G PER GLI OPERATORI TELCO

16 maggio 2022 – In un mondo ormai digitale che si espande giorno dopo giorno, in cui persone, oggetti –Internet of Things, aziende sono costantemente connessi e dialogano tra loro in tempo reale, la connettività veloce sarà sempre più essenziale, tanto quanto il cloud computing. Ecco perché la tecnologia 5G è destinata a cambiare come mai prima d'ora il mondo delle telecomunicazioni. Non solo dal punto di vista tecnico, ma anche di business, con un'importante espansione del mercato di riferimento. Il 5G rappresenta la rete di connessione della "quarta rivoluzione industriale". Grazie alla maggior ampiezza di banda, il 5G permette di fare leva su una velocità di trasmissione dati senza precedenti, con un consumo di energia significativamente inferiore. Si diffonderanno, quindi, nuove tecnologie che hanno bisogno di sfruttare un'alta velocità di trasmissione di grandi volumi di traffico dati a bassa latenza.
(source: https://www.lineaedp.it/news/62200/il-cloud-computing-elemento-chiave-della-tecnologia-5g-per-gli-operatori-telco/)

BOLLINO CYBER. IL DECRETO PER CERTIFICARE LA SICUREZZA TECH

04 maggio 2022 – In Cdm il decreto legislativo che adegua l'Italia alla normativa Ue sulla certificazione cyber. L'Agenzia di Baldoni diventa l'ente responsabile, i prodotti Tic dovranno avere un "bollino" di garanzia. Un tassello in più per mettere al sicuro la Pa da ingerenze esterne, dal 5G cinese ai software russi.
(source: https://formiche.net/2022/05/bollino-cyber-draghi/)

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

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

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

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.