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

Newsletter

ANNO 2022 | N. 04 | APRILE

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

BLOCKCHAIN SECURITY:

come garantire la sicurezza informatica della Blockchain

Nell'editoriale di marzo abbiamo parlato di come la blockchain possa essere utilizzata in favore della Cybersecurity, tuttavia la Blockchain, come qualsiasi tecnologia IT scritta in codice di programmazione, è a sua volta soggetta a tipologie di manomissioni e manipolazioni e come tale ha bisogno di essere soggetta a pratiche di sicurezza informatica per evitare che sia danneggiata. Infatti, qualsiasi tecnologia può contribuire ad aumentare la superficie di attacco e d è solo questione di tempo prima che gli attaccanti trovino una falla o una vulnerabilità da poter sfruttare non solo a livello di codice, ma a livello di processo applicativo, fino a spingersi al livello utente solitamente molto più semplice da raggirare.

La blockchain security è quella serie di prassi applicate per rendere sicura la tecnologia di blockchain. In altri termini e nella logica di valutazione del rischio di sicurezza, la blockchain security è una procedura completa di valutazione del rischio eseguita per una soluzione o una rete blockchain per garantirne la sicurezza. La protezione si ottiene attraverso l'implementazione di framework di sicurezza informatica, metodologie di test di sicurezza e pratiche di codifica sicure per proteggerla da frodi online, violazioni e altri tipi di attacchi informatici. Ma vediamo i casi più frequenti di attacchi alle blockchain e quali sono le prassi per la prevenzione.

Gli **attacchi, di tipo "51%",** sono effettuati da miner malevoli che potrebbero prendere riunire risorse sufficienti per acquisire più del 50% della potenza di mining di una rete blockchain. Ovvero un miner malevolo potrebbe raccogliere più della metà dell'hash rate e prendere il controllo dell'intero sistema. In tal modo l'attaccante può modificare l'ordine delle transazioni e impedirne la conferma, annullare le transazioni precedentemente completate, con conseguente doppia spesa. Questo tipo di attacchi colpisce solo le blockchain pubbliche e non quelle private. La **prevenzione per questi attacchi consiste nelle prassi** di miglioramento del monitoraggio del pool di mining; adozione di un hash rate maggiore del normale; valutazione dei pro e contro delle procedure di consenso proof-of-work (PoW) e Proof of Stake (PoS) per scegliere in modo da minimizzare il rischio di miner malevoli.

Gli **Attacchi Sybil** perpetrati mediante inondazione della rete bersaglio con una quantità schiacciante di false identità, mandando in crash il sistema. In altre parole, gli hacker generano numerosi nodi di rete falsi. Utilizzando questi nodi, l'hacker può ottenere il

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

consenso della maggioranza e interrompere le transazioni della catena o inondarla. Di conseguenza, un assalto di Sybil su larga scala non è altro che un attacco del 51% o una sorta di DDOS. La **prevenzione per questi attacchi consiste nelle prassi** di utilizzo di algoritmi di consenso appropriati; monitoraggio del comportamento di altri nodi e verifica della presenza di nodi che inoltrano blocchi solo da un utente.

Gli **Attacchi di routing** (o attacchi diretti) sono effettuati verso i provider di servizi internet (ISP) per intercettare direttamente i dati trasferiti dalle blockchain, mediante account anonimi, senza che gli utenti blockchain possano accorgersi di problemi (estrazione di valuta o esposizione di dati riservati). La **prevenzione per questi attacchi consiste nelle prassi** di implementazione di protocolli di routing sicuri mediante certificati; utilizzo della crittografia dei dati; modifica regolare delle password e scelta di password complesse.

La **vulnerabilità degli endpoint della blockchain** è un altro importante problema di sicurezza. L'endpoint della rete blockchain è il punto in cui gli utenti interagiscono e può essere costituito da computer e/o da telefoni cellulari. Gli hacker possono osservare il comportamento degli utenti e prendere di mira i dispositivi per rubare la chiave dell'utente. La **prevenzione per questi attacchi richiede** di evitare di salvare le chiavi blockchain sul proprio computer o cellulare come file di testo; sono inoltre consigliate prassi standard di revisione regolare del dispositivo tenendo traccia dell'ora, della posizione e dell'accesso al dispositivo e installazione di antivirus e software anti-malware.

Anche le blockchain a livello utente possono soffrire di **attacchi di phishing**. Obiettivo dell'hacker in un attacco di phishing è rubare le credenziali dell'utente (collegate a cryptowallets). L'e-mail dall'aspetto legittimo invita l'utente a inserire i dettagli di accesso tramite un collegamento ipertestuale falso allegato. La **prevenzione per questi attacchi consiste nelle prassi di protezione verso gli endpoint usati dall'utente** e quindi riguarda prassi note ma che è preferibile ripetere: riconferma della mail ricevuta utilizzando un altro canale di contatto con il mittente(se lo si conosce) e scartando la mail se non si conosce il mittente; ottimizzazione della sicurezza del browser installando un componente aggiuntivo verificato per essere avvisati di siti Web non sicuri; evitare sempre di selezionare il collegamento prima di averlo esaminato a fondo. L'eventuale passaggio e verifica del link mediante il browser è consigliabile se e solo sul browser è stata predisposta opportuna configurazione e componenti di sicurezza; aumento della sicurezza del dispositivo installando un software di rilevamento dei collegamenti dannosi e un software antivirus affidabile; aggiornamento puntuale del sistema e dei software del dispositivo; evitare le reti Wi-Fi aperte quando utilizzi un portafoglio elettronico o altre importanti transazioni bancarie; adottare soluzioni antiphishing.

In caso di utilizzo della blockchain come asset aziendale (blockchain privata) sono consigliate alcune prassi a livello dell'impresa:

1. Definire i ruoli di accesso per monitorare l'accesso dei dipendenti in base ai ruoli nell'organizzazione.
2. Implementare accessi e autenticazione multi-fattore
3. Garantire la sicurezza dello Smart contract; lo Smart Contract è un programma che risiede nella blockchain e viene eseguito al verificarsi di alcune condizioni predeterminate. In altre parole, è un modo conveniente per approvare una transazione. Si consiglia di verificare quindi le "condizioni predeterminate" (Responsabilità, Titolarità e segregazione dei compiti) in modo puntuale.
4. La gestione delle chiavi di sicurezza nell'organizzazione richiede di stabilire politiche e procedure apposite per evitare manomissioni e sottrazioni delle stesse.
5. Definire la Privacy Policy della Blockchain in termini di policy sull'l'integrità dei dati e delle modalità con cui è mantenuta in tutta la Blockchain.
6. Garantire la network security dell'impresa perché la blockchain è connessa in rete

Infine, è utile ricordare un "sempreverde" della prevenzione: la formazione e la spiegazione dei fenomeni criminali gli utenti della Blockchain, per far comprendere e capire come agisce la minaccia, per aumentare la consapevolezza e la preparazione degli utenti apportando un grande beneficio di lungo termine.

Alessia Valentini
Cyber security consultant, CISA

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

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.
- 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!

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

CSX-P™

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:

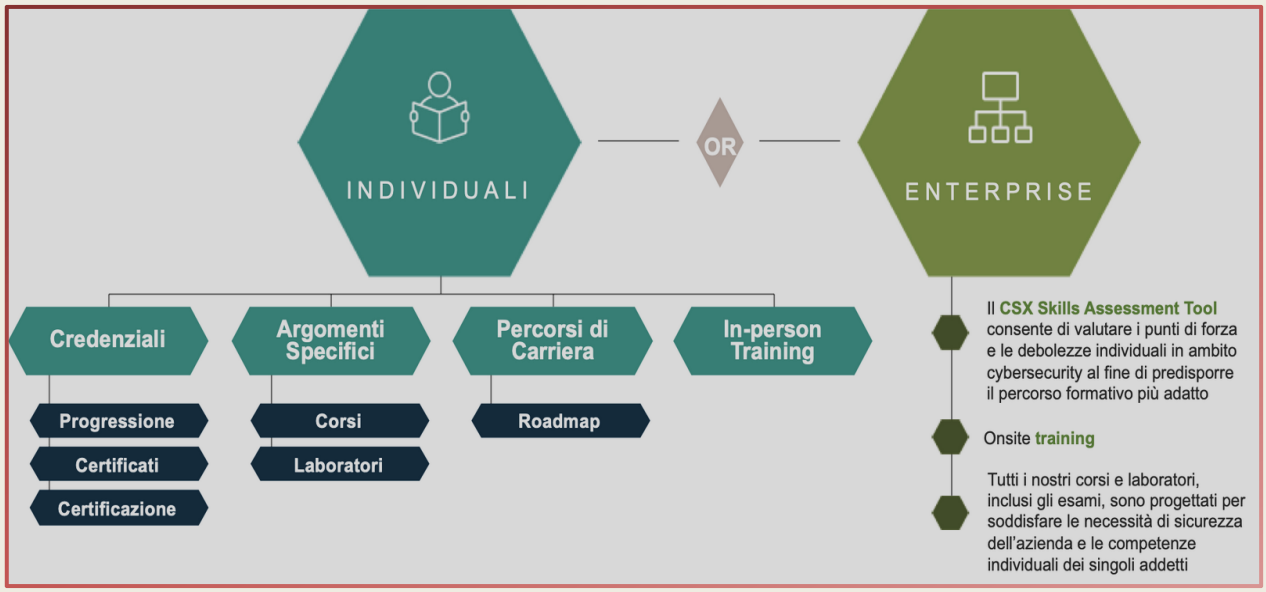
- **Laboratori on-line** – Laboratori realizzati da ISACA International e fruibili come parte integrante dei nostri corsi.
- **Laboratori specialistici esclusivi** – In aggiunta a quelli offerti da ISACA il nostro team di specialisti in ambito cybersecurity e sistemistico ha sviluppato una serie di laboratori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

29 MARZO 2022

"SICUREZZA DELLE FUNIVIE E SICUREZZA CIBERNETICA: IL PERCHÉ DI UN APPROCCIO INTEGRATO"

Un sistema di trasporto a fune è sistema "cyber-fisico" in cui componenti elettronici programmabili sono incorporati nella parte strutturale, elettrica e meccanica. È un sistema complesso con notevoli interazioni con gli operatori e soprattutto con gli utenti, che avviene attraverso componenti fondamentali quali l'azionamento, i sistemi di frenatura, i sistemi meccanici di linea, i veicoli. Anche nei sistemi di trasporto a fune si intende trarre i benefici della IoT e delle tecnologie elettroniche e digitali per il miglioramento della gestione e dell'esperienza degli utenti. Tali benefici, tuttavia, hanno degli aspetti da valutare accuratamente in quanto introducono delle nuove vulnerabilità, soprattutto a fronte di tecniche di attacco "cyber" mirate che possono essere anche molto sofisticate.

Guardando alle eventuali conseguenze che attacchi possono avere, il concetto di "cybersecurity" si estende da quello tipicamente inteso relativamente all'information tecnology fino a toccare l'affidabilità, la manutenibilità e la safety dei sistemi di trasporto a fune. Il webinar, a partire da una descrizione funzionale di un impianto a fune, approfondirà questi aspetti, mettendo in risalto l'importanza di integrare le valutazioni relative alla sicurezza funzionale delle funivie con quelle relative alla cyber-security, ricorrendo a specifiche tecniche di analisi.

Relatore: Ing. Giorgio Pizzi

Laureato in Ingegneria Elettronica con esperienza su sistemi medicali, impianti elettrici, gestione e sicurezza di reti e sistemi informatici. Dal 2010 è dirigente del MIMS. Dal 2013 al 2021 è stato Direttore dell'Ufficio per la vigilanza sulla sicurezza di metropolitane, tramvie, ferrovie locali, impianti a fune, filovie, ascensori e scale mobili in servizio pubblico nel Centro-Nord Italia. Dalla fine del 2020 è Dirigente presso la Direzione Generale per il trasporto pubblico locale e regionale, con competenze su impianti a fune, scale mobili e ascensori, e digitalizzazione del trasporto. È componente del Comitato Tecnico Permanente per la sicurezza dei sistemi di trasporto ad impianti fissi e della Commissione per le Funicolari Aeree e Terrestri. Tra i suoi interessi ci sono l'integrazione tra safety e cybersecurity con particolare riguardo ai sistemi di trasporto, e le piattaforme digitali, soprattutto quelle per la mobilità.

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);*

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

- *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

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

GUERRA, LE SEI ISTRUZIONI ALLE PA DALL'AGENZIA CYBERSICUREZZA NAZIONALE

26 aprile 2022 – Istruzioni precise alle pubbliche amministrazioni per cambiare le soluzioni dedicate alla sicurezza degli end-point e al firewall che venivano fornite da provider legati alla Russia, i quali **potrebbero non essere in grado di fornire aggiornamenti e soluzioni a causa della guerra in Ucraina**, con possibili ripercussioni di sicurezza.
Si tratta di **sei best practice**da attuare per evitare rischi, contenute nella circolare numero 4336 del 21 aprile 2022 dell'*Agenzia per la cybersicurezza nazionale* in attuazione dell'articolo 29, comma 3 del cosiddetto Decreto Ucraina, cioè il decreto numero 21 del 21 marzo 2022.
La norma prevede infatti che le PA sostituiscano i prodotti di sicurezza informatica di operatori legati alla Russia, in quanto, a causa del conflitto in corso, i provider potrebbero non aver la possibilità di **"fornire servizi e aggiornamenti ai propri prodotti"**, si legge nella *nella circolare pubblicata in Gazzetta Ufficiale il 26 aprile*.
(source: https://www.cybersecurity360.it/news/guerra-le-sei-indicazioni-per-le-pa-dellagenzia-cybersicurezza-nazionale/)

GDPR, BELLO E IMPOSSIBILE

22 aprile 2022 – Quasi impossibile rispettare il Gdpr al 100%, ma le imprese devono cercare in buona fede la strada migliore per rispettare la privacy. Così Secondo Sabbioni, Data Protection Officer dal 2012 del Parlamento europeo, per il quale la collaborazione tra istituzioni e operatori economici è la chiave del successo delle norme sulla protezione dei dati, che non mancano, però, di chiaroscuri.
A un quarto di secolo dall'inizio dell'era italiana della privacy (l'8 maggio 1997 entrava in vigore il grosso della legge 675/1996, la prima legge sulla riservatezza) è tempo di fare il punto della situazione. Ma in una prospettiva europea.

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

(source: https://www.italiaoggi.it/news/gdpr-bello-e-impossibile-2559923)

LAPSUS$ HACKERS TARGETED T-MOBILE SOURCE CODE IN LATEST DATA BREACH

22 aprile 2022 – The *Lapsus$ hacking group* has claimed another victim: U.S. telecom giant T-Mobile.
T-Mobile's latest security incident — the seventh data breach in the past four years — was *first revealed* by security journalist Brian Krebs, who obtained a week's worth of private chat messages between the core members of Lapsus$, a hacking and extortion group that gained notoriety in recent months after targeting tech giants *Nvidia*, *Ubisoft* and *Okta*. The messages obtained by Krebs were sent in a private Telegram channel during the week leading up to *the arrests of the gang's most active members* in March. At least two Lapsus$ members — a 16-year-old and a 17-year-old — *were subsequently charged with multiple cyber offenses*.
(source: https://tcrn.ch/3MliYN6)

QUATTRO ITALIANI SU 10 NON SI DIFENDONO DAI CYBER ATTACCHI

22 aprile 2022 – Il 28,1% degli italiani è preoccupato per la sicurezza informatica ma non fa nulla di concreto per difendersi mentre il 10,3% non ha alcuna preoccupazione in materia: in pratica, **quattro italiani su 10 sono indifesi da eventuali cyber attacchi**, "un ventre molle pericoloso, fatto di bersagli facili, potenziali gate di ingresso per cyber-criminali". È quanto emerge dal primo "Rapporto Censis-DeepCyber sul valore della cybersecurity", presentato oggi nella Sala Zuccari del Senato.
(source: https://www.agi.it/cronaca/news/2022-04-23/quattro-italiani-su-dieci-nessuna-difesa-cyber-attacchi-16468967/)

TUTTE LE MOSSE DELLA CINA PER RUBARE DATI COMMERCIALI (E NON SOLO)

24 aprile 2022 – Diversi paesi, tra cui Paesi Bassi, Regno Unito, Australia e Stati Uniti, e aziende come Vodafone e Microsoft hanno rivelato la campagna senza sosta della Cina per rubare dati commerciali e altri dati sensibili.
La Cina sfrutta le vulnerabilità del software di posta elettronica di Microsoft per prendere di mira i dipartimenti del governo degli Stati Uniti, gli appaltatori della difesa, i gruppi di riflessione sulle politiche e i ricercatori sulle malattie infettive, tra gli altri.
(source: https://www.startmag.it/mondo/cina-furto-dati-commerciali/)

GABRIELLI: «ATTACCHI HACKER IN ITALIA? AL MOMENTO LE NOSTRE STRUTTURE SONO TROPPO FRAGILI»

24 aprile 2022 – Un chiarimento, a cui tiene molto. E un'invocazione, che gli sta ancora più a cuore. **Franco Gabrielli, sottosegretario alla presidenza del Consiglio e Autorità delegata per la sicurezza della Repubblica**, è fiero per la nascita dell'**Agenzia per la cybersicurezza nazionale** ma, allo stesso tempo, vuole ribadire che questa non è «la panacea di tutti i mali, non abbiamo risolto ogni problema. Dopo attacchi informatici come quello alle Ferrovie, ci siamo sentiti domandare: "Ma l'Agenzia non doveva proteggerci?". È il solito tentativo di dare risposte semplificate a problemi complessi». Ecco perché Gabrielli ci tiene a sottolineare che l'Agenzia per la cybersicurezza nazionale (Acn) è nata «per far sì che questo **Paese si doti di un sistema più resiliente del dominio cibernetico, ma tutto ciò presuppone un percorso, che stiamo costruendo**». Uno sviluppo, quindi, da cui scaturisce l'invocazione «verso **un'indipendenza tecnologica che non può essere soltanto nazionale ma va immaginata in una dimensione europea**. Perché nessun Paese dispone da solo di questa autonomia, nemmeno le superpotenze».
(source: https://www.corriere.it/tecnologia/22_aprile_24/gabrielli-attacchi-hacker-italia-nostre-strutture-sono-troppo-fragili-6ca2324c-c3d9-11ec-b866-99e8752a9d0f.shtml)

PROGETTARE IL FUTURO DEI DATI E DELLA VITA

23 aprile 2022 – Partiamo da un assunto: come tutte le cose di questo universo in cui vige un sistema entropico, le informazioni, biologiche o digitali, durano solamente finché c'è qualcuno che se ne prende cura.
Non c'è insieme di standard che offra garanzie ragionevolmente sufficienti sul fatto che le informazioni archiviate saranno ancora accessibili tra qualche decennio da ora. L'unico modo in cui il nostro archivio (o il nostro corpo) può rimanere attivo è se verrà continuamente aggiornato e adattato al futuro. Se un archivio rimane ignorato, alla fine diventerà inaccessibile.
(source: https://www.uomoemanager.it/progettare-il-futuro-dei-dati-e-della-vita/)

VALUTAZIONE D'IMPATTO PRIVACY: PUBBLICARE O NON PUBBLICARE?

24 aprile 2022 – Per quanto si possa dire della *modalità di conduzione* della valutazione d'impatto, dunque del *coinvolgimento degli interessati*, nelle organizzazioni che vogliono essere conformi al GDPR c'è sempre il dubbio circa la pubblicazione di una sintesi o degli esiti della stessa. Come ricorda l'EDPB (WP 248), sebbene non sussista alcun obbligo derivante dal GDPR, "*pubblicarne una sintesi potrebbe favorire la fiducia*" che è un elemento fondamentale per la relazione con l'interessato, al fine di riequilibrare – quanto meno relativamente all'aspetto della trasparenza informativa – il rapporto con gli interessati consentendo agli stessi un maggiore grado di coinvolgimento e partecipazione effettiva.
(source: https://www.infosec.news/2022/04/24/news/riservatezza-dei-dati/valutazione-dimpatto-privacy-pubblicare-o-non-pubblicare/)

CYBERSICUREZZA: IN 7 GIORNI L'ITALIA HA SUBITO 35 CAMPAGNE MALEVOLE

25 aprile 2022 – La **cybersicurezza** è ormai diventato un tema sensibile a tutti. Chiunque naviga in internet, possiede uno o più indirizzi email, accede ai suoi social network o ha un account con il quale gestisce i suoi dispositivi dovrebbe proteggere la sua **privacy** e i suoi **dati**.
Infatti, in soli 7 giorni, il **CERT-AGID**, team impegnato nella tutela nazionale in ambito di **cybersicurezza**, ha registrato ben **35 campagne malevole**.
(source: https://www.telefonino.net/notizie/cybersicurezza-in-7-giorni-italia-subito-35-campagne-malevole/)

CYBERSECURITY, LA SFIDA NELLA SFIDA

27 aprile 2022 – La cybersecurity è ormai un elemento e tema sempre più preminente, non solo per l'agenda europea, ma anche per quella italiana. Prima per gli effetti della pandemia, ora per quelli della guerra in Ucraina, gli attacchi cyber si stanno

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

intensificando. Emerge quanto non adottare strategie cyber adeguate possa esporre le aziende e il territorio in cui esse operano a rischi elevati. Del tema abbiamo parlato con **Fabio Momola, COO Gruppo Engineering, CEO D.Hub & Cybertech**, azienda fondata in Italia nel 2007 con il nome di OmnitechIT, poi divenuta Cybertech nel 2019 e da gennaio 2022 controllata al 100% dal Gruppo Engineering. Negli anni è diventata un operatore di riferimento nella cybersecurity, registrando una crescita significativa fino a raggiungere lo scorso anno 29 milioni di euro di ricavi.
(source: https://www.startupbusiness.it/cybersecurity-la-sfida-nella-sfida/118587/)

COSA SONO GLI ATTACCHI "ZERO DAY" E PERCHÉ SONO SEMPRE PIÙ DIFFUSI

25 aprile 2022 – Le cosiddette **vulnerabilità "*zero-day*"** precedentemente sconosciute all'interno dei software sono un concetto misterioso e intrigante. Sono però ancora più degne di nota quando vengono individuati criminali informatici che sfruttano le nuove falle di un software prima che chiunque altro ne sia a conoscenza. Dal momento che i ricercatori hanno aumentato gli sforzi per rilevarli e studiarli, gli attacchi di questo tipo stanno venendo alla luce con **maggiore frequenza**. Questa settimana **due rapporti** realizzati dalla società di *cybersecurity Mandiant* e dal team di *Google* che si occupa di scovare i bug, *Project Zero*, cercano di fornire un quadro più preciso su quanto esattamente gli attacchi zero-day siano cresciuti negli ultimi anni.
(source: https://www.wired.it/article/cybersecurity-attacchi-zero-day/)

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**

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

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

CISA Certified Information Systems Auditor. An ISACA® Certification

CRISC Certified in Risk and Information Systems Control. An ISACA® Certification

CISM Certified Information Security Manager. An ISACA® Certification

CGEIT Certified in the Governance of Enterprise IT. An ISACA® Certification

CSX-P CSX Cybersecurity Practitioner. An ISACA® Certification

CDPSE Certified Data Privacy Solutions Engineer. An ISACA® Certification

ITCA Information Technology Certified Associate An ISACA® Certification

CYBER SECURITY AUDIT An ISACA Certificate

COBIT An ISACA® Framework

CSX CYBERSECURITY NEXUS

IT RISK FUNDAMENTALS An ISACA Certificate

CCAK Certificate of Cloud Auditing Knowledge A Cloud Security Alliance® and ISACA® Credential

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.