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

Newsletter

ANNO 2022 | N. 01 | GENNAIO

ISACA (Information Systems Audit and Control Association)

L'ISACA, (Information Systems Audit and Control Association), ha 158.300 associati in oltre 188 nazioni (dato aggiornato a 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

LOG4J: IL BILANCIO A UN MESE DAL TERREMOTO DIGITALE

Con il nuovo anno non si placa il terremoto digitale causato dalla scoperta della vulnerabilità Log4shell del tool di logging Log4j, usato in moltissimi siti web e applicativi basati su Java. Tracciamo quindi un bilancio della situazione a un mese di distanza dall'accaduto.

La cronistoria della vulnerabilità inizia il 10 dicembre con la sua scoperta nel gioco Minecraft, ma quasi immediatamente la si riscontra quasi ovunque su Internet: i server di Amazon, Apple e Microsoft si rivelano vulnerabili nonostante *l'impegno del produttore Apache per la risoluzione* con le prime patch sulla falla in qualità di creatore di Log4j.

La vulnerabilità classificata come CVE-2021-44228, ha avuto un rating di gravità pari a 10/10 e sembra fosse nota agli esperti e addetti ai lavori della sicurezza informatica già da qualche giorno prima, ovvero dai primissimi giorni dello scorso dicembre. Log4Shell è di fatto una vulnerabilità zero-day, in Log4j, che permette l'esecuzione di codice arbitrario. In particolare, la vulnerabilità sfrutta le richieste di Log4j a server LDAP e JNDI arbitrari, consentendo agli aggressori di eseguire codice Java arbitrario su un server o un altro computer o di divulgare informazioni riservate. La complessità e gravità è dovuta al fatto che Log4J è un componente piccolo che monitora e registra eventi, azioni, utente di routine errori, segnalandoli agli amministratori di sistema, e come tale, è molto diffuso sia nei prodotti e sia, per ereditarietà (dipendenze indirette), all'interno di progetti più grandi. *La direttrice della CISA Jen Easterly la considera la più grave mai vista* e spiega che le dipendenze sono rischiose a causa delle vulnerabilità nascoste in profondità nella rete interconnessa di software. Quindi a causa dell'enorme numero di progetti software correlati e interessati dalla vulnerabilità, Log4Shell è stata indicata come la più grave vulnerabilità degli ultimi anni, anche rispetto al noto *Heartbleed* del 2014. Di fatto dopo appena due settimane dalla disclosure gli attacchi criminali legati a Log4Shell sono stati circa 3.7 milioni con conseguenti danni milionari, fughe di dati a colpi di botnet e ransomware. Ma *una recente ricerca di JFrog* sulle dipendenze indirette del codice, stima danni per ancora diversi anni con incidenze dolorose per le supply chain del Software. In questo senso un altro recente sfruttamento della vulnerabilità Log4shell è stato evidenziato sul *prodotto VMware Horizon*.

Alcune *patch sono state rilasciate sia da Apache* sia da altri vendor che avevano adottato il tool Log4j, tuttavia, non tutte le aziende interessate dal problema sono state in grado di applicare la patch a Log4j, ad esempio, in presenza di applicazioni Saas in Cloud o applicazioni Custom per cui la patch va personalizzata. Questi soggetti si sono trovati quindi ad un bivio: disattivare l'applicazione colpita, smettere di

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

usarla e, a seguire, ripensare l'intera componente informatica interessata, oppure assumersi il rischio, nella speranza di non essere colpiti dai criminali e di ricevere correttivi dalle entità istituzionali. In questo senso le autorità statunitensi, Federal Trade Commission (FTC) e Cybersecurity and infrastructure security agency (CISA) sono intervenute. La CISA ha fissato la scadenza ad appena prima dello scorso Natale chiedendo alle aziende di scoprire se hanno usato Log4j nei loro sistemi e di applicare una patch. Per questo ha pubblicato una *guida, ovvero una procedura in cinque step* e un diagramma algoritmico per valutare la propria condizione di vulnerabilità aziendale. La FTC invece, ai primi di Gennaio, ha emesso *un avviso urgente per la remediation* del problema pena l'applicazione di sanzioni.
La sequenza di scansioni automatizzate verso i bersagli vulnerabili e l'ondata di attacchi che si sono susseguiti da Dicembre, è proseguita fino ai primi di gennaio come testimoniano i dati del Cert Agid riportati nella *sintesi riepilogativa degli attacchi fino al 7 Gennaio* di quest'anno. Sul sito del Cert Agid è anche presente una *lista aggiornata al 12 Gennaio di tutti gli IoC per la mitigazione,* mentre sul sito del CSIRT italiano è stata dedicata una *intera pagina a Log4shell e a tutti gli ALERT per le sue mitigazioni*.

La Apache Software foundation ha infine rilasciato (fonte "*The Hacker News*") la versione 2.17.0 di Log4j, contenente la terza patch risolutiva della falla Log4Shellc che dovrebbe essere immune sia alla vulnerabilità CVE-2021-45105, (per le versioni dalla 2.0 beta9 alla 2.16.0), sia alla vulnerabilità CVE-2021-44228, più propriamente nota come Log4Shell.

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.
- 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

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

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:

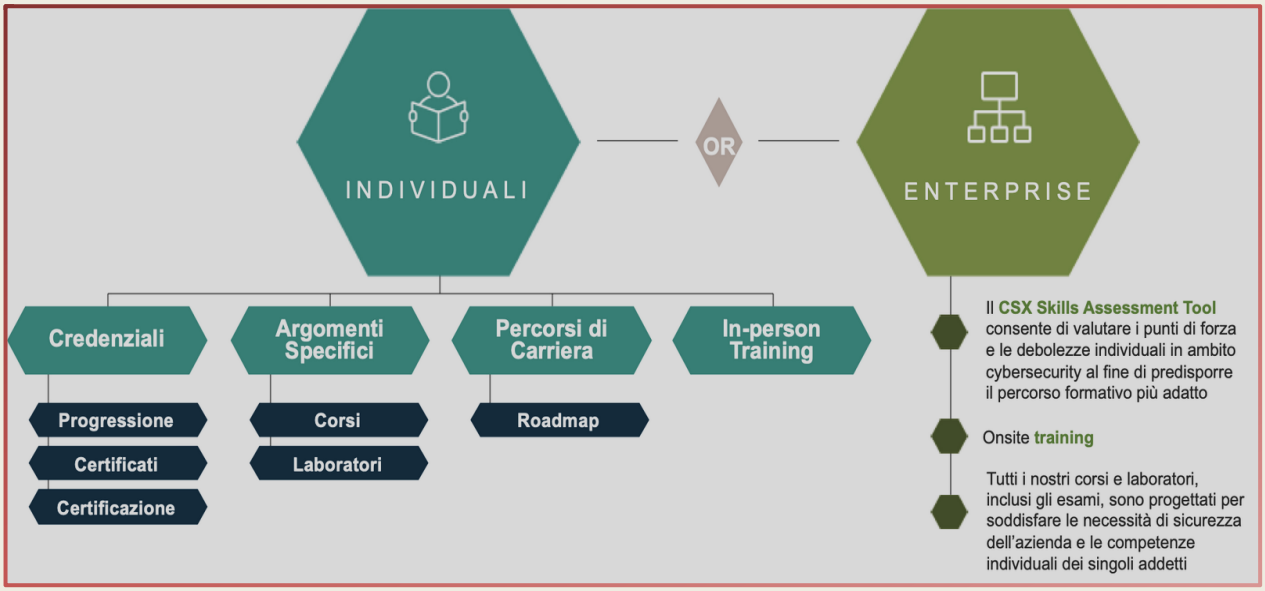
- **Laboratori on-line** – Laboratori realizzati da ISACA International e fruibili come parte integrante dei nostri corsi.
- **Laboratori specialistici esclusivi** – In aggiunta a quelli offerti da ISACA il nostro team di specialisti in ambito cybersecurity e sistemistico ha sviluppato una serie di laboratori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

WEBINAR
RINVIATO A METÀ GENNAIO 2022

"HACKING DALLE ORIGINI ALLA FIGURA PROFESSIONALE DELL'ETHICAL HACKER, ACCENNI ALLE METODOLOGIE INTERNAZIONALI, REGOLE DI INGAGGIO E NORMATIVA NAZIONALE"

Parleremo di:

Le origini dell'Hacker: dalle incursioni per sfida al rischio di "bruciarsi". L'esperienza sul campo e l'evoluzione. Ethical hacker metodologie internazionali, regole di ingaggio. Normativa nazionale e problematiche legali.

Ci sarà una tavola rotonda e la possibilità di interlocuzione con i relatori

Ne parleranno:

Massimilano Graziani

Stefano Aterno

E altri……stiamo preparando un paio di sorprese…Ci aiuterà come giornalista ***Alessia Valentini***

Massimiliano Graziani dopo aver prestato servizio dell'Aeronautica Militare ha seguito la sua vocazione per l'informatica e nel 1992 ha fondato la Cobra Soft, azienda di sviluppo software con la quale ha colto moltissimi primati in ambito di Hacking & Countermeasures, come ad esempio il primo test comparativo sugli antivirus pubblicato in Italia. Dal 2005, si è dedicato completamente agli aspetti della sicurezza, fondando insieme ad altri il capitolo italiano dell'OWASP. Come dipendente ha svolto il ruolo di Manager di area sulla sicurezza IT, in varie aziende di informatica. Ha quindi fondato la sua attuale azienda CYBERA SRL. Dal 2005 ha iniziato una lunga collaborazione, che prosegue con sempre maggiore intensità, con le Procure e Forze dell'Ordine in ambito della Computer Forensics. È socio fondatore e membro di numerose associazioni. Ha numerose e prestigiose certificazioni in ambito cybersec e cyber forensic. Ha svolto e svolge continuamente numerosi corsi e seminari presso le FF.OO , organismi giudiziari, università

Stefano Aterno Avvocato esperto di diritto delle nuove tecnologie, Cassazionista, Professore presso Università di Foggia, l'Università RomaTRE e la Luiss Guido Carli University. Insegna diritto alla protezione dei dati personali, Data protection e aspetti giuridici della sicurezza informatica in alcune Università italiane presso il Dipartimento di Giurisprudenza ed in particolare all'Università di Foggia, all'Università di RomaTRE, e alla Luiss. Inoltre è docente in diversi Master universitari di I e II livello dedicati all'insegnamento del diritto delle nuove tecnologie e della sicurezza informatica. Già Direttore del Corso di diritto penale dell'informatica e diritto delle nuove tecnologie della Lumsa di Roma. Esperto di legislazione in materia di cybercrime, aspetti giuridici della Computer forensics, di indagini difensive informatiche; legislazione sulla privacy, sul trattamento dei dati personali e Regolamento europeo n. 679/2016 (GDPR), AI e diritto, Robotica e Responsabilità contrattuale ed extracontrattuale. Socio dello Studio Legale E-Lex. Certificato ISO 27001 Lead Auditor (Pecb Montreal Canada) dal 2012. Certificato Uni 11697: 2017 Data Protection Officer dal 2020. Certified Information Forensics Investigator, (CIFI). Consulente di aziende private, multinazionali e pubblica amministrazione.

Alessia Valentini Consulente di Cybersecurity, Advisor e Giornalista. Attualmente in Gruppo Daman svolge attività di Advisor, Business Developer e Consulente di Cybersecurity. Fa parte delle "Women for Security" la community di Cyberladies nata nell'ambito del Clusit. È Giornalista presso l'ODG del Lazio dal 2013.

Come giornalista si occupa di News Analysis, Brand Blogging e Brand Journalism per Cybersecurity 360 – digital 360 e di interviste e articoli per StartUpItalia! (precedentemente HTML.iT del gruppo Triboo Media, Flyorbitnews) occupandosi trattando di temi legati alla Cybersecurity, open-innovation, start-up e best practices per le PMI, l'imprenditorialità in rosa e per favorire la partecipazione femminile nelle discipline STEM e nella Cybersecurity. Collabora con il gruppo redazionale del capitolo di ROMA dell'ISACA per scrivere gli editoriali della newsletter mensile. Ha conseguito la certificazione CISA /ISACA nel 2017. È stata consigliere direttivo in Afcea (Armed Forces Electronic Association) dal 2014 al 2016 per la divulgazione e il supporto tecnico per gli approfondimenti tematici della forza armata ed ha partecipato ai lavori

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

dell'Osservatorio Sicurezza Nazionale presso il CASD fino al 2013. In ambito internazionale ha svolto il ruolo di Direttore Tecnico del progetto Europeo POSEID-ON (Protection and COntrol of Secured Information by means of a privacy Enhanced Dashboard), Manager tecnico nel progetto Europeo CyberROAD dedicato allo sviluppo di una roadmap europea per il contrasto al Cybercrime e Cyberterrorismo e come Responsabile Dissemination per il progetto PREEMPTIVE, per la protezione delle infrastrutture critiche di tipo SCADA.

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

LOG4SHELL: LA VULNERABILITÀ HA GIÀ RAGGIUNTO IL LIVELLO DI GRAVITÀ 10/10

14 dicembre 2021 – Sono passati solo quattro giorni dalla scoperta della vulnerabilità Log4Shell del tool di logging Log4j, usato in moltissimi siti web e applicativi basati su Java. **La vulnerabilità è stata scoperta su Minecraft**, ma nel giro di poche ore gli analisti hanno riscontrato la sua presenza praticamente ovunque su Internet.

(source: https://tech.everyeye.it/notizie/log4shell-vulnerabilita-raggiunto-livello-gravita-10-10-558456.html)

SINTESI RIEPILOGATIVA DELLE CAMPAGNE MALEVOLE NELLA SETTIMANA DEL 01 – 07 GENNAIO 2022

07 gennaio 2022 – In questa settimana, il CERT-AGID ha riscontrato ed analizzato, nello scenario italiano di suo riferimento, un totale di 20 campagne malevole di cui 19 con obiettivi italiani ed una generica che ha comunque interessato l'Italia, mettendo a disposizione dei suoi enti accreditati i relativi 138 indicatori di compromissione (IOC) individuati.

(source: https://cert-agid.gov.it/news/sintesi-riepilogativa-delle-campagne-malevole-nella-settimana-del-01-07-gennaio-2022 /)

CERT-AGID CONDIVIDE GLI IOC PER LA MITIGAZIONE DEGLI ATTACCHI LOG4SHELL

17 gennaio 2022 – Come evidenziato anche dal CSIRT Italia, la vulnerabilità censita come CVE-2021-44228 riguardante Apache Log4j sta creando notevoli problemi di sicurezza sui sistemi esposti che utilizzano quel prodotto.

Il CERT-AGID, a protezione delle proprie infrastrutture e di quelle della sua constituency, sta raggruppando gli IoC (Indicatori di Compromissione) pubblici individuati dalle comunità di ricercatori di sicurezza (che in questi giorni si stanno adoperando per mitigare i danni di questa grave vulnerabilità) oltre a quelli che riesce a rilevare dai vari log delle proprie infrastrutture, per poterli utilizzare come contrasto alle ondate di scansioni che si stanno verificando al fine di sfruttare questa vulnerabilità.

(source: https://cert-agid.gov.it/news/cert-agid-condivide-i-propri-ioc-per-la-mitigazione-degli-attacchi-log4shell/)

CHAOS RANSOMWARE, IL RANSOMWARE "ITALIANO" CHE SI NASCONDE TRA I REFERTI DELLA POLIZIA DI STATO

18 gennaio 2022 – È stata identificata una variante di Chaos Ransomware con chiara matrice italiana: il malware sfrutta finti referti della Polizia di Stato per attirare le vittime in trappola e, purtroppo, pagare il riscatto serve a poco perché i file di dimensione superiore a 2 MB vengono irrimediabilmente cancellati. Ecco tutti i dettagli e i consigli per difendersi.

(source: https://www.cybersecurity360.it/nuove-minacce/ransomware/chaos-ransomware-il-ransomware-italiano-che-si-nasconde-tra-i-referti-della-polizia-di-stato/)

DATA BREACH, LE NUOVE LINEE GUIDA EDPB SULLA NOTIFICA: FOCUS SUL "RISCHIO UMANO"

17 gennaio 2022 – Adottate a fine dicembre, le nuove linee guida sugli esempi di notifica degli episodi di data breach forniscono una guida pratica e concreta, oltre a una serie di raccomandazioni, nella fase di gestione del data breach e della valutazione

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

del rischio connesso allo stesso. Analizzati anche una serie di case studies.
(source: https://www.agendadigitale.eu/sicurezza/privacy/data-breach-le-nuove-linee-guida-edpb-sulla-notifica-focus-sul-rischio-umano/)

COME FUNZIONA LA CENTRALE OPERATIVA PER LA CYBERSECURITY DELLA POLIZIA

17 gennaio 2022 – Il concetto di big data è da anni sempre più al centro delle nostre vite, ma quando si pensa alla raccolta di dati sensibili è più comune prendere in considerazione quelle messe in atto dalle cosiddette big tech come Meta e Google, piuttosto che quelle delle forze dell'ordine. Anche queste ultime però raccolgono enormi quantità di dati particolarmente sensibili, come dimostrato in questi giorni dal provvedimento del garante europeo della protezione dei dati contro l'Europol.
A gestire questa categoria di dati in Italia, dallo scorso aprile c'è il Cybersecurity operations center (C-Soc), una sala operativa che fa capo all'Ufficio protezione dati della Polizia di Stato. Wired ha raggiunto il suo direttore Stefano Moni, il procurement manager Giuseppe Restivo e il project manager Francesco Talone per capire da cosa è composto e come funziona il C-Soc..
(source: https://www.wired.it/article/cybersecurity-operations-center-polizia-come-funziona/)

CYBERCRIME, 40 CAMPAGNE CONTRO L'ITALIA LA SCORSA SETTIMANA

17 gennaio 2022 – Il CERT-AgID: L'Italia è stata vittima di 40 campagne la settimana scorsa. Usati i malware AgentTesla, Emotet, Formbook, Ursnif/Gozi, Brata, sLoad, Avemaria e Lokibot. Il phishing ha preso di mira soprattutto le banche.
(source: https://www.difesaesicurezza.com/cyber/cybercrime-40-campagne-contro-litalia-la-scorsa-settimana/)

ENERGIA, TEMA DI SICUREZZA NAZIONALE: ECCO PERCHÉ SCENDE IN CAMPO IL COPASIR

13 gennaio 2022 – Il Comitato sui Servizi: l'Italia deve realizzare un piano nazionale di sicurezza nazionale in modo che possa restare valido ed indirizzare le scelte strategiche che il Paese.
(source: https://www.lastampa.it/cronaca/2022/01/13/news/energia_tema_di_sicurezza_nazionale_ecco_perche_scende_in_campo_il_copasir-2827546/)

WHY DATA OPERATIONS PLATFORMS CAN'T SURVIVE WITHOUT GOVERNANCE

18 gennaio 2022 – Data operations (DataOps) is a data management methodology that improves an organization's efficiency and profitability by applying agile techniques to the workflows that derive business value from data. It leverages a combination of processes and technologies to reduce data friction, improve business agility, and increase security, integrity, and reliability throughout the data pipeline. However, to achieve increased productivity, a DataOps system has to ensure that the data is governed throughout its life cycle as it moves through increasingly complex pipelines and analytics workflows.
(source: https://tdwi.org/articles/2022/01/18/biz-all-why-data-operations-platforms-cant-survive-without-governance.aspx)

CYBERSECURITY E OSPEDALI: METÀ DEI DEVICE CONNESSI A INTERNET È A RISCHIO

20 gennaio 2022 – Negli ultimi mesi, gli attacchi hacker sono diventati una seria *minaccia di cybersecurity per gli ospedali*, che ormai da qualche anno vengono **spesso colpiti dai ransomware rilasciati da gruppi di cybercriminali**, che così facendo però mettono a rischio i dati e, soprattutto, la vita dei pazienti.
(source: https://tech.everyeye.it/notizie/cybersecurity-ospedali-meta-device-connessi-internet-rischio-565006.html)

I DATA BREACH IN EUROPA SONO AUMENTATI DELL'8% NEL 2021

19 gennaio 2022 – I dati dei cittadini europei non si possono dire propriamente al sicuro. Le notifiche di data breach sono infatti aumentate dell'8% nei paesi dell'Unione europea lo scorso anno rispetto al precedente, per un totale di oltre 130mila violazioni dei dati personali. Dal 28 gennaio 2021 a oggi i garanti privacy europei hanno inoltre inflitto sanzioni per più di un miliardo di euro, come conseguenza di una vasta gamma di violazioni al Regolamento generale europeo sulla protezione dei dati (Gdpr).
(source: https://www.wired.it/article/dati-data-breach-europa-aumento/)

MULTE PER OLTRE UN MILIARDO DI EURO DAL GDPR

19 gennaio 2022 – Aumento impressionante di sanzioni per violazione del Gdpr. Nel 2021 le multe per violazione della privacy sono costate alle imprese 1,1 miliardi di euro, rispetto ai 272,5 milioni del 2020. A rivelarlo, lo studio legale DlaPiper nel suo report annuale "General data protection regulation (Gdpr) fines and data breach survey" condotto nei paesi dell'UE più Uk, Norvegia, Islanda e Liechtenstein.
(source: https://www.smartworld.it/internet/multe-per-oltre-un-miliardo-di-euro-dal-gdpr.html)

A CYBERATTACK ON A RED CROSS CONTACTOR RESULTED IN THE THEFT OF PERSONAL DATA FOR MORE THAN 515,000 HIGHLY VULNERABLE PEOPLE

20 gennaio 2022 – La crescita esponenziale di dispositivi IoT collegati alle reti degli operatori tlc e alle infrastrutture cloud, procedono di pari passo con lo sviluppo delle reti 5G necessarie per la loro diffusione. Questo scenario sta creando un ambiente ricco di insidie di cybersecurity, specie con l'evoluzione verso la smart factory.
(source: https://www.agendadigitale.eu/sicurezza/cybersecurity-i-rischi-di-5g-e-iot-per-le-smart-factory-il-ruolo-delle-telco-e-gli-scenari/)

CARO ENERGIA, IN GIOCO LA SICUREZZA NAZIONALE: L'ALLARME DEL COPASIR

20 gennaio 2022 – Transizione energetica e caro energia sono al centro della Relazione sulla sicurezza energetica nell'attuale fase di transizione ecologica" del Copasir. Rischi, criticità e fragilità che destano allarme
(source: https://www.agendadigitale.eu/smart-city/caro-energia-in-gioco-la-sicurezza-nazionale-lallarme-del-copasir/)

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

http://www.isacaroma.it/

Social Media

SAPIENZA
UNIVERSITÀ DI ROMA

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

CISA, CRISC, CISM, CGEIT, CSX-P O CDPSE DOPO IL TUO NOME DIMOSTRA CHE HAI LE COMPETENZE PER AFFRONTARE LE SFIDE DELL'AZIENDA MODERNA:

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

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