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

Newsletter

ANNO 2022 | N. 03 | MARZO

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

la tecnologia di protezione, gli sviluppi

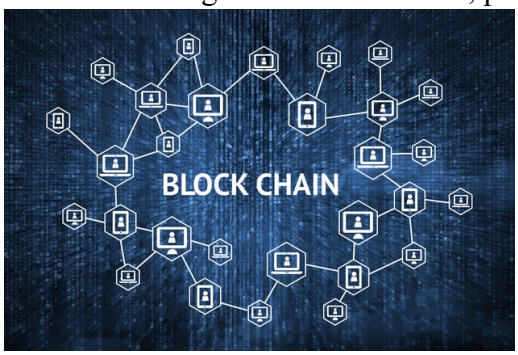
Si parla molto di blockchain, o meglio se ne parla di nuovo, dopo una prima ondata di entusiasmo che dal 2018 in poi, aveva portato la tecnologia blockchain alla ribalta di quasi ogni progetto IT. Alzi la mano chi in quel periodo non ha sentito almeno una delle possibili applicazioni della blockchain senza che fosse spiegato in dettaglio il suo funzionamento e perché proprio questa tecnologia fosse adatta per quella applicazione piuttosto che altre. Come sempre anche nell'IT ci sono "le mode", le tendenze e dal 2018 con parte del 2019 sembrava che la blockchain fosse la panacea di ogni problema. Si ricorda anche il famoso *gruppo di esperti del MISE* per la definizione di un *documento di strategia, oggi pubblicato per la pubblica consultazione* chiusa a fine 2020. Ma dal 2020 in poi, forse complice anche la pandemia, la Blockchain è "caduta nel dimenticatoio" e solo oggi si assiste a timidi revamping. Anche *l'Europa si è dedicata a questa tecnologia con una strategia specifica* nell'ambito della più ampia strategia per la Digital Europe. Ci occupiamo quindi di questa tematica per il doppio ruolo che concorre a giocare con la Cybersecurity. Come per ogni tecnologia IT, **la Blockchain può essere vista sia come abilitante per garantire aspetti di sicurezza informatica (blocco 1), ma a sua volta necessita di essere soggetta a buone prassi di sicurezza informatica (blocco 2)**. Questo ci ricorda il famoso *paradosso del barbiere di Bertrand Russell* ma rifrasato: chi chi protegge la tecnologia di sicurezza?

Ripartiamo dalla definizione di blockchain analizzando come la blockchain possa garantire sicurezza e i suoi sviluppi futuri. Nella prossima newsletter ci occuperemo di come proteggere la Blockchain.

Le tecnologie Blockchain sono incluse nella più ampia famiglia delle tecnologie di Distributed Ledger (si rimanda a *definizione tecnica di Distributed Ledger e Blockchain* per gli approfondimenti), ossia sistemi che si basano su un registro distribuito, che può essere letto e modificato da più nodi di una rete. Per validare le modifiche da effettuare al registro, in assenza di un ente centrale, i nodi devono raggiungere il consenso. Le modalità con cui si raggiunge il consenso e la struttura del registro sono alcune delle caratteristiche che connotano le diverse tecnologie Distributed Ledger (Fonte *Osservatori.net*). In sostanza, la Blockchain è una tecnologia che consente a utenti e organizzazioni di archiviare ed elaborare dati con i blocchi distribuiti strutturati presenti in una rete. Ogni nuovo blocco memorizza una transazione o un pacchetto di transazioni che è collegato a tutti i blocchi precedentemente di-

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

sponibili sotto forma di catena crittografica. La tecnologia Blockchain è anche considerata come un sistema di contabilità distribuito e decentralizzato in grado di registrare transazioni tra più computer.
Si ricordano a puro titolo di completezza le tre tipologie di blockchain: Pubblica, Privata e consorziata. Le blockchain del primo tipo sono completamente trasparenti, il che implica che chiunque può analizzare i dettagli della transazione, nel secondo tipo le transazioni che avvengono su blockchain private sono private e sono semplicemente accessibili ai membri del sistema a cui è stato permesso di unirsi alla rete. Il terzo tipo è simile al secondo ma le blockchain del consorzio non sono governate da un'unica entità, sono governate da un gruppo. I partecipanti alle blockchain del consorzio potrebbero incorporare chiunque, dalle banche nazionali ai governi, alle catene di approvvigionamento.
Le prime applicazioni della blockchain e il risalto mediatico sono stati collegati all'uso della tecnologia come base del Bitcoin, ma quasi subito è stata considerata una **promettente tecnologia di mitigazione per la sicurezza informatica** grazie alle sue capacità di indicare qualsiasi comportamento scorretto e di fornire certezza nell'integrità delle transazioni. La blockchain garantisce alcuni prerequisiti di progettazione che la rendono intrinsecamente sicura per cui spesso viene definita Secure-by-design:



1. Decentralizzazione: i dati contenuti nella blockchain sono decentralizzati e verificati; quindi, se un sistema è correttamente distribuito si elimina il concetto di single point of failure.
2. Anti-tampering: la struttura blockchain con il tempo si fortifica man mano che si aggiungono blocchi. Questo perché al crescere della struttura è sempre più difficile spezzare la catena dei consensi e prendere il controllo della struttura dati, per cui la manomissione dei dati in Blockchain è quasi impossibile
3. Zero proof knowledge: concetto che riguarda la protezione dati. Il sistema di blockchain nell'ambito della gestione delle identità digitali permette di accertare che una certa persona sia chi dice, che abbia certi requisiti, senza dire chi è.
4. Memorizza i dati applicando algoritmi di crittografia
5. La blockchain è trasparente: Il contenuto del registro è trasparente e visibile a tutti ed è facilmente consultabile e verificabile (questo influisce sulla privacy dei dati)
6. Tracciabilità: Ciascun elemento sul registro è tracciabile in ogni sua parte e se ne può risalire all'esatta provenienza

Grazie a queste caratteristiche la blockchain può essere utile nell'autenticazione di device OT e IOT ad una rete e nella capacità di capire se un certo device è integro o no. Questa tecnologia automatizza completamente l'archiviazione dei dati, riducendo l'elemento umano in questi sistemi di archiviazione dei dati e diminuendo di conseguenza la probabilità di errore umano. Può essere utilizzata in qualsiasi settore o industria, perché qualsiasi tipo di asset o transazione digitale di qualsiasi settore può essere inserito in una rete a blocchi. Tipicamente sono state implementate applicazioni alla tracciabilità alimentare e dei prodotti da filiera controllata come anche del "made in italy".
Di recente invece la tecnologia blockchain è legata al *WEB 3 Project,* ovvero la terza generazione del Web che dovrebbe essere una crypto-internet fondata sulla blockchain. e dovrebbe garantire agli utenti la massima libertà d'uso togliendo alle big tech la possibilità di controllarlo. Mirella CAstiglie. Alessandro Longo spiegano che "*L'idea è che se il Web 1.0 è stato sito con contenuti non modificabili dall'utente, e il web 2.0 ha portato ai contenuti generati dagli utenti, ora con il 3.0 si vorrebbe (o si dice che si vorrebbe) dare agli utenti il controllo stesso dei servizi e dell'infrastrutture alla base*".

Alessia Valentini
Cyber security consultant, CISA

NOVITA' DAL CAPITOLO

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

ACCORDO

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:

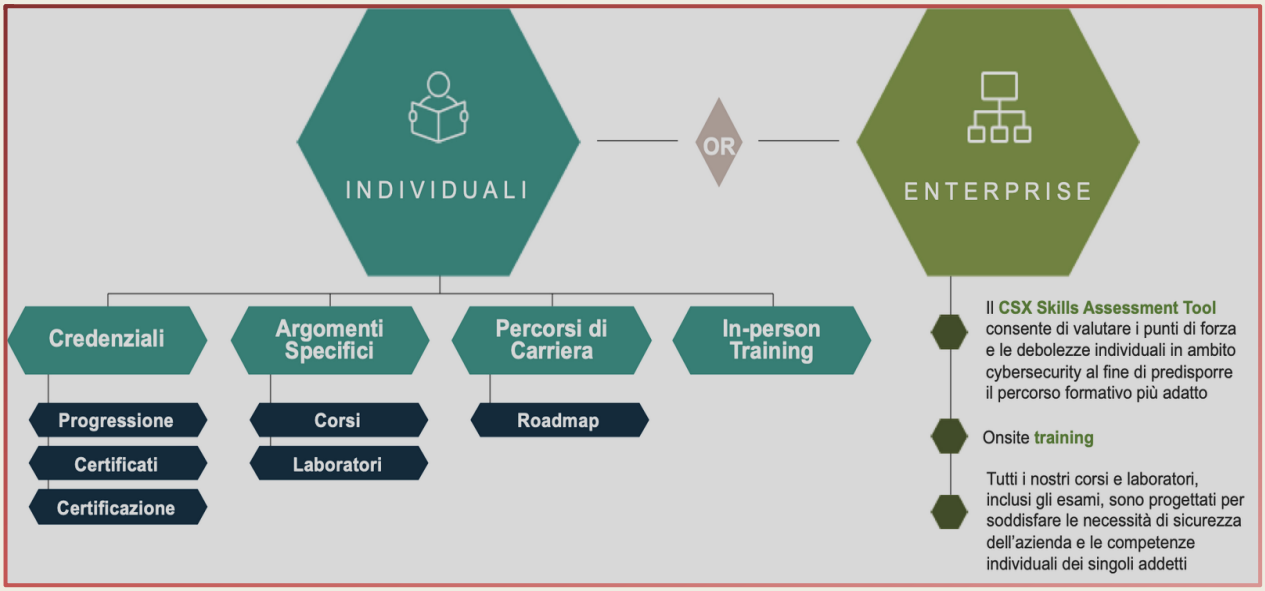
- **Laboratori on-line** – Laboratori realizzati da ISACA International e fruibili come parte integrante dei nostri corsi.
- **Laboratori specialistici esclusivi** – In aggiunta a quelli offerti da ISACA il nostro team di specialisti in ambito cybersecurity e sistemistico ha sviluppato una serie di laboratori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

14 GENNAIO 2022 — "HACKING DALLE ORIGINI ALLA FIGURA PROFESSIONALE DELL'ETHICAL HACKER, ACCENNI ALLE METODOLOGIE INTERNAZIONALI, REGOLE DI INGAGGIO E NORMATIVA NAZIONALE"

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.

Massimilano Graziani

Stefano Aterno

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.

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

PROSSIMI EVENTI

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

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

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.

venerdì 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

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

VIA L'ANTIVIRUS KASPERSKY DALLA PUBBLICA AMMINISTRAZIONE, LA CONFERMA NEL DECRETO UCRAINA

21 marzo 2022 – *Come vi abbiamo riportato la scorsa settimana*, **Franco Gabrielli**, ex capo della polizia e della Protezione Civile e che ora ricopre la carica di sottosegretario alla presidenza del Consiglio con delega alla sicurezza nazionale, intervistato dal *Corriere della Sera* aveva espresso la propria preoccupazione inerente all'impiego di software prodotti in Russia, soprattutto nei sistemi della **Pubblica Amministrazione**. In particolare, si era fatto riferimento al popolare **antivirus Kaspersky** che, come affermato da Cybersecurity Italia a *Il Tempo*, viene impiegato ampiamente da oltre 2.200 enti pubblici, tanto che il software potrebbe essere presente anche sul computer di Mario Draghi, presidente del consiglio.
(source: https://www.tomshw.it/hardware/via-lantivirus-kaspersky-dalla-pubblica-amministrazione-la-conferma-nel-decreto-ucraina/)

IL DECRETO "KASPERSKY" E LA NECESSITÀ DI RAFFORZARE LA NOSTRA SOVRANITÀ DIGITALE

22 marzo 2022 – Il cosiddetto decreto "Kaspersky" è la risposta alla crisi ucraina che ha, di fatto, costretto il governo ad adottare misure urgenti volte a rafforzare la sovranità tecnologica e digitale dell'Italia, anche nell'ambito della cyber security. Ecco quali scenari si aprono adesso.
(source: https://www.cybersecurity360.it/outlook/il-decreto-kaspersky-e-la-necessita-di-rafforzare-la-nostra-sovranita-digitale/)

CLUSIT, FAGGIOLI: "RISCHIO CYBER ALTO PER AZIENDE E PA, SERVONO SCELTE FORTI IN EUROPA"

21 marzo 2022 – "Necessario attenersi alle disposizioni del Csirt per incrementare preventivamente il livello di protezione. Le politiche siano univoche a livello comunitario". L'allarme del Mit: "L'isolamento digitale della Russia potrebbe cambiare per sempre il Web"
(source: https://www.corrierecomunicazioni.it/cyber-security/clusit-faggioli-rischio-cyber-alto-per-aziende-e-pa-servono-scelte-forti-in-europa/)

GOLDEN POWER, LA PROPOSTA ALLA LUCE DELLA GUERRA IN UCRAINA: TRE LINEE DI INTERVENTO RAPIDO

22 marzo 2022 – Riflettendo sull'estensione del decreto Golden Power, la priorità è pensare a una strategia di difesa nazionale capillare da applicare in un contesto di escalation militare, per poter implementare le attività di cyber security in modo repentino coinvolgendo tutta la comunità, a tutela delle infrastrutture critiche e di quelle a esse collegate.
(source: https://www.cybersecurity360.it/cybersecurity-nazionale/golden-power-la-proposta-alla-luce-della-guerra-in-ucraina-tre-linee-di-intervento-rapido/)

UN "BOLLINO" PER LA CYBERSECURITY MADE IN UE: L'INIZIATIVA ECSO

23 marzo 2022 – La "Cybersecurity Made in Europe Label" promossa da ECSO (European Cyber Security Organization) permetterà alle aziende di entrare in una lista di fornitori di alta qualità e garantirà loro riconoscibilità verso clienti, partner commerciali e potenziali investitori. Requisiti e benefici per le aziende col "bollino".
(source: https://www.agendadigitale.eu/sicurezza/un-bollino-per-la-cybersecurity-made-in-ue-liniziativa-ecso/)

TRENITALIA, ANCORA IN TILT IL SISTEMA INFORMATICO. SPUNTA LA MATRICE CRIMINALE

24 marzo 2022 – Nessun riscatto chiesto a seguito dell'*attacco informatico a Fs* e nessun collegamento certo con gli hacker russi. Lo chiarisce il Gruppo Ferrovie dello Stato. "Le aziende del Gruppo Fs Italiane non hanno ricevuto richieste di riscatto dopo l'attacco hacker", si puntualizza, evidenziando che "allo stato attuale non sussistono elementi che consentano di risalire all'origine e alla nazionalità dell'attacco informatico".
Ferrovie dello Stato sta lavorando in stretta collaborazione con l'Agenzia per la Cybersicurezza Nazionale e con la Polizia di Stato. "In particolare, il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (Cnaipic) della Polizia Postale è impegnato a condurre tutti gli adeguati controlli e verifiche su quanto accaduto oggi – si legge – La circolazione ferroviaria prosegue regolarmente e i sistemi di vendita nelle stazioni (biglietterie e self service) sono stati inibiti soltanto per motivi di sicurezza, mentre gli altri sistemi online sono operativi. I viaggiatori sprovvisti di biglietto saranno regolarizzati a bordo treno senza sovrapprezzo".
(source: https://www.corrierecomunicazioni.it/digital-economy/trenitalia-ancora-in-tilt-il-sistema-informatico-spunta-la-matrice-criminale/)

POLITICA INTERNA PRIVACY: ECCO COME GARANTIRE SICUREZZA DEI PROCESSI AZIENDALI E COMPETITIVITÀ

25 marzo 2022 – Il GDPR non contiene norme precettive ma un "framework normativo" che fissa solo principi e requisiti,

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

senza indicare le modalità per realizzarli/soddisfarli, lasciando ad ogni organizzazione la responsabilità di allestire una politica interna volta a integrare i principi della protezione dei dati personali nei processi aziendali. Ecco come.
(source: https://www.cybersecurity360.it/legal/privacy-dati-personali/politica-interna-privacy-ecco-come-garantire-sicurezza-dei-processi-aziendali-e-competitivita/)

CYBERSECURITY: AUMENTANO GLI INVESTIMENTI IN ITALIA

26 marzo 2022 – Con l'aumento dello smart working sono aumentati anche gli attacchi informatici, per questo molte imprese italiane hanno intrapreso o potenziato gli investimenti nella cybersecurity. Secondo quanto riportato da Ansa, il ***mercato della cybersecurity*** in Italia ha raggiunto i 1,55 miliardi di euro, registrando una **crescita del +13%** rispetto al 2020.
Nonostante questo, però il rapporto tra spesa in sicurezza e Pil resta limitato (0,08%), posizionandosi all'ultimo posto tra i Paesi del G7.
(source: https://www.corrierenazionale.it/2022/03/26/cybersecurity-aumentano-gli-investimenti-in-italia/)

CYBERSECURITY, POCA SPESA E TROPPI RISCHI: ECCO PERCHÉ L'ITALIA È IN PERICOLO

28 marzo 2022 – Secondo l'Osservatorio del PoliMI, il rapporto tra spesa in Cybersecurity e PIL nazionale resta limitato (0,08%).
(source: https://www.economymagazine.it/cybersecurity-poca-spesa-e-troppi-rischi-ecco-perche-litalia-e-in-pericolo/)

HEALTH DATA BREACHES SWELL IN 2021 AMID HACKING SURGE, POLITICO ANALYSIS FINDS

23 marzo 2022 – Nearly 50 million people in the U.S. had their sensitive health data breached in 2021, a threefold increase in three years, according to a POLITICO analysis of the latest HHS data.
Health care organizations including providers and insurers in every state except South Dakota reported such incidents last year. About half of states and Washington, D.C., saw more than 1 in 10 of their residents directly impacted by unauthorized access to their health information, according to the analysis. And hacking accounted for nearly 75 percent of all such breaches — up from 35 percent in 2016.
(source: https://www.politico.com/news/2022/03/23/health-data-breaches-2021-hacking-surge-politico-00019283)

AN INTEGRATED APPROACH TO SECURITY AUDITS

23 marzo 2022 – A cyberattack can be devastating to any organization because it compromises sensitive data and, as a result, the financial position, strategic vision, and more important, the trust and credibility that the enterprise has built over the years. Given the magnitude of this risk, what role does the IT security audit function play in minimizing the risk likelihood and impact? And why is it important to adopt an integrated approach to IT and security auditing? Finding ways to leverage controls and testing across multiple frameworks can save organizations time and effort during audits while giving a more holistic view of their audit, compliance and security postures.
(source: https://www.isaca.org/resources/news-and-trends/industry-news/2022/an-integrated-approach-to-security-audits)

GLOBAL CYBERSECURITY RAMIFICATIONS FROM THE WAR IN UKRAINE

20 marzo 2022 – What are the most important trends in global cybersecurity? How are current events impacting the wider cyber conflicts and incidents that public- and private-sector organizations face every day? How will these events shape the world in the years ahead in cyberspace?
These questions are becoming more and more difficult to answer as new alliances are being formed as a result of the war in Ukraine. Back when we started the year, the *top cyber experts and companies made numerous predictions regarding cybersecurity in 2022*, but no one predicted what is happening now.
(source: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/global-cybersecurity-ramifications-from-the-war-in-ukraine)

GLI STATI UNITI HANNO MESSO L'ANTIVIRUS KASPERSKY NELLA LISTA NERA

28 marzo 2022 – *La società russa di cybersicurezza* ***Kaspersky Lab*** è stata inserita nella *lista* degli enti che rappresentano un ***"rischio inaccettabile per la sicurezza nazionale degli Stati Uniti"***, come conseguenza dell'*invasione dell'Ucraina* voluta dal presidente russo Vladimir Putin. Una mossa ulteriore che mette all'angolo l'azienda dell'omonimo antivirus, tra i migliori sul mercato. Nelle ultime settimane, **Francia, Germania e Italia hanno già intrapreso azioni contro Kaspersky**, raccomandando agli utenti di sostituirlo con altre applicazioni, per evitare di esporre enti pubblici o aziende ad attacchi informatici.
(source: https://www.wired.it/article/kaspersky-antivirus-lista-nera-minaccia-sicurezza-nazionale-stati-uniti/)

SITI INTERNET E SERVIZI PA: LE LINEE GUIDA AGID OCCASIONE IMPORTANTE PER LA DATA PROTECTION

29 marzo 2022 – Le linee guida AgID, una volta aggiornate con le indicazioni del Garante, saranno finalmente occasione per ripensare i processi di ogni PA, sia quelli relativi alle piattaforme digitali che quelli interni, di modo da mettere al centro la tutela dei dati personali di ogni cittadino italiano. Ecco come.
(source: https://www.agendadigitale.eu/cittadinanza-digitale/siti-internet-e-servizi-pa-le-linee-guida-agid-occasione-importante-per-la-data-protection/)

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

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 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.