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

Newsletter

ANNO 2022 | N. 07 | LUGLIO-AGOSTO

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

FOCUS ON CREDENTIAL STUFFING ATTACKS

Già nel 2020 l'FBI lanciava segnali di allarme per il numero crescente di *attacchi di Credential Stuffing contro le istituzioni finanziarie*. Anche se il termine è emerso prima del 2010, data in cui ha iniziato ad essere osservato dai laboratori dei vendor che monitorano la minaccia, si tratta di un termine relativamente nuovo, che indica un tipo di attacco automatizzato in cui i criminali digitali sfruttano le raccolte di nomi utente e password che sono trapelati online tramite violazioni di dati presso altre società e li provano contro account di altri servizi online. Tale termine si usa anche quando gli attaccanti identificano gli account in cui gli utenti hanno riutilizzato le stesse password già compromesse e le usano quindi per ottenere l'accesso non autorizzato al profilo dell'utente e alle risorse allegate. Dopo l'accesso possono verificarsi vari scenari: esfiltrazione di dati e/o di denaro dai conti acceduti, acquisti per conto della vittima, accesso ad informazioni sensibili quali carte di credito, messaggi privati, immagini o documenti da rivendere nel dark web, ulteriore utilizzo dell'account per inviare messaggi di phishing o di spam, fino alla rivendita delle credenziali "validate" su uno o più siti compromessi per l'utilizzo da parte di altri aggressori.
All'epoca della loro identificazione gli attacchi di Credential Stuffing non sembravano diffusi, ma sono diventati una piaga alla fine degli anni 2010 poiché nei cinque anni precedenti gli attaccanti avevano raccolto miliardi di combinazioni di nomi utente e password trapelati online da centinaia di aziende. Anche oggi, secondo l'*Application Protection Report* a cura degli F5 Labs, il livello degli attacchi che derivano dalla compromissione della posta elettronica aziendale è sottostimato anche se rappresenta il 24% di tutte le violazioni. Infatti, questa tipologia di violazione viene spesso riferita con pochissimi dettagli, a parte il fatto che le e-mail dei dipendenti sono state compromesse, e porta alla considerazione che il vero peso di Credential Stuffing sia oggi ancora sottostimato; si consideri anche che la compromissione degli accessi si conferma come il punto di ingresso principale delle violazioni e come primo passo di compromissione per molte altre catene di attacco.
Il maggior successo e diffusione si deve all'uso dell'automazione da parte degli attaccanti. Inizialmente gli attaccanti erano costretti a introdurre manualmente il nome e utente e password per ogni sito da violare e quindi la capacità di danneggiamento era in qualche modo limitata. Invece il ricorso a bot per l'automazione e la scalabilità dell'attacco, consente il riempimento delle credenziali con l'iniezione automatizzata di coppie di nome utente e password rubate ("credenziali") nei moduli di accesso al sito Web, ciò ottimizza e velocizza l'accesso fraudolento agli account utente. Gli attaccanti sono inoltre facilitati dalla

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

pessima abitudine degli utenti di riusare la stessa password e nome utente/e-mail su siti e servizi digitali diversi, anzi vi fanno affidamento come presupposto; quando le credenziali di questo tipo di utenti "disattenti" sono esposte (ad esempio a causa di una violazione del database o di un attacco di phishing) l'invio di tali set di credenziali rubate a dozzine o centinaia di altri siti può consentire a un utente malintenzionato di compromettere anche quegli account.
Il *rapporto Cost of Credential Stuffing del Ponemon Institute* ha rilevato che le aziende perdono in media 6 milioni di dollari all'anno a causa del Credential Stuffing sotto forma di downtime delle applicazioni, perdita di clienti e aumento dei costi IT. In aggiunta possono insistere le multe dell'autorità Garante per i dati personali in tutti i casi in cui le aziende possono essere soggette ad azioni legali ai sensi delle leggi sulla privacy dei dati (GDPR) se non implementano misure di sicurezza adeguate a prevenire tali attacchi, non informano il pubblico di una violazione o non fanno abbastanza per proteggere le password. Esempi significativi sono stati quelli del 2018, in cui l'Information Commissioner's Office (ICO) del Regno Unito ha multato Uber £ 385.000 per "una serie di falle evitabili nella sicurezza dei dati" che hanno esposto i dati di circa 2,7 milioni di clienti del Regno Unito, mentre nel 2021, l'Autorità francese per la protezione dei dati (CNIL) ha multato un titolare del trattamento e il suo responsabile del trattamento di € 225.000 "per la mancata adozione di misure di sicurezza adeguate per proteggere i dati personali dei clienti dagli attacchi di Credential Stuffing sul sito Web del titolare del trattamento" (Fonte *Auth0*).
Rilevare un attacco Credential Stuffing attuato da bot automatiche è complesso tanto più che gli effetti sono visibili quando ormai il maggior danno è avvenuto. *Deepak Gupta esperto di sicurezza* suggerisce di prestare attenzione a tre segnali: verificare la presenza di modifiche nel traffico del sito come tentativi di accesso multipli su più account, entro un periodo di tempo limitato; non trascurare mai i casi d'uso in cui si assiste a un tasso di errore di accesso superiore al normale; prestare attenzione a eventuali tempi di inattività registrati causati da un aumento del traffico del sito. In aggiunta si rendono necessarie protezioni aggiuntive per lo screening e arresto dei bot e una tecnologia di screening e rilevamento di malware sui dispositivi.

Il Credential Stuffing può essere considerato come un sottoinsieme della categoria degli attacchi di forza bruta; la "brutalità" consiste proprio nei tentativi automatizzati di provare più password contro uno o più account al fine di indovinarla. (fonte *OWASP*) Tuttavia mentre negli attacchi a forza bruta l'introduzione di password robuste e di multifactor authentication può garantire protezione, nel Credential Stuffing l'uso di una password complessa non impedirà a un criminale informatico di accedere a un account perché la password è già nota. Invece l'autenticazione a più fattori rappresenta la contromisura principale; in particolar per prevenire il Credential Stuffing può essere consigliabile adottare:

- **Autenticazione senza password:** che impedisce il riempimento delle credenziali perché verifica un utente con qualcosa che ha (un dispositivo o un altro account) o qualcosa che è (biometria) invece di una password (qualcosa che conosce). Generalmente questo metodo di autenticazione è percepito migliore per gli utenti e consente alle organizzazioni di risparmiare tempo e denaro nell'affrontare la reimpostazione della password.
- **Autenticazione continua:** i sistemi di autenticazione continua utilizzano fattori biometrici o modelli comportamentali per verificare l'identità di un utente in tempo reale (mentre utilizza un'applicazione) piuttosto che una password.
- **Autenticazione a più fattori (MFA):** l'autenticazione a più fattori (MFA) previene il riempimento delle credenziali perché richiede agli utenti di accedere con un'altra forma di autenticazione oltre a una combinazione nome utente-password.
- **Hashing delle credenziali:** l'hashing cripta la password di un utente prima della memorizzazione nel database in modo che, in caso di furto, un attaccante non possa usarla (o meglio non possa usarla immediatamente, perché gli attaccanti potrebbero provare a decriptare i dati, ma almeno in questo lasso temporale la vittima ha il tempo utile per cambiar le proprie credenziali n.d.r.)
- **Formazione specifica** per aumentare la consapevolezza su questo tipo di attacco e sulle buone prassi di gestione degli accessi ai propri siti, applicazioni, sociale etc.

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

Per un approfondimento sulle tecniche di difesa si consigli di fare riferimento al documento OWASP *Credential Stuffing Prevention cheat sheet* e ai consigli di *difesa di Anastasios Arampatzis* ufficiale di forza armata (Aeronautica) ed esperto IT e Cybersecurity in contesti NATO ed EU.

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 stiamo proseguendo con lo svolgimento di eventi on-line. Le modalità di informazione sono le consuete mail di annuncio/invito spedite ai contatti della nostra mailing-list che coincide con la diffusione della Newsletter. Per iscriversi alla mailing list è sufficiente inviare una mail con oggetto SUBSCRIBE a *eventi@isacaroma.it*.
Vi terremo informati su eventuali eventi in presenza, per il momento vi auguriamo buona lettura!

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).

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.

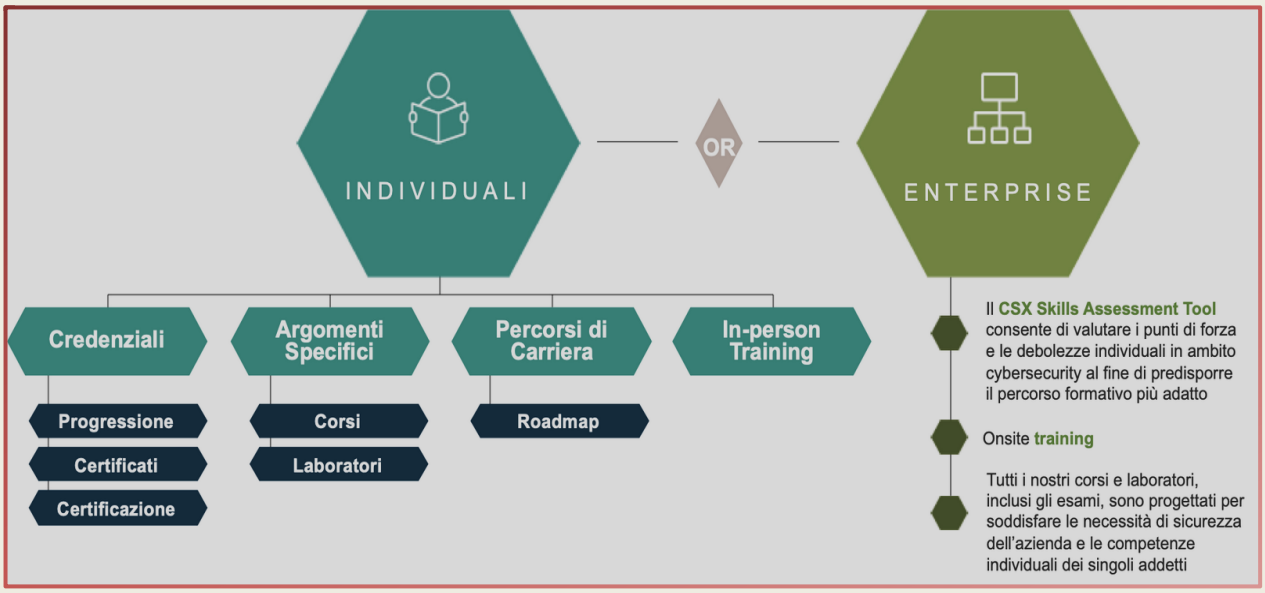
È stato anche realizzato un laboratorio permanente per sessioni di Cyber Range. L'attività comprende simulazioni di rete ed esercizi di attacchi che permettono ai professionisti della sicurezza di potenziare competenze, esperienza, efficacia, comunicazione e processi.

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.

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



Maggiori dettagli sono disponibili*about:blank* 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

EVENTI PASSATI

VEN 01 LUGLIO 2022
ORE 15:00-17:00

"INSERT COIN TO CONTINUE... IL RANSOMWARE NEL GAMING"

"Un recente ingaggio nel mondo del gaming online mi ha introdotto ad alcune pratiche proprie di questa industria che, se da un lato applica stringenti controlli applicativi, dall'altra sembra essere piuttosto rilassata nei confronti della gestione delle infrastrutture... come mi ha potuto dimostrare una famosa gang di ransomware..."

Il relatore: ***Stefano Maccaglia***
È Senior Principal Consultant nel team di Incident Response di RSA dal 2012 e ha alle spalle numerose investigazioni su incidenti di grandi dimensioni in varie parti del mondo. Hacker della prima ora, nonche' antropologo e sociologo, nel suo percorso lavorativo ha collaborato con molte realta' di primo piano del panorama ICT mondiale, da Digital a Cisco. Speaker abituale di conferenze internazionali, al di fuori del lavoro e' attivo nella produzione di contributi sulle tematiche della cybersecurity e del cyber-spionaggio.

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

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

PROSSIMI EVENTI

16 Settembre 2022
ore 15,00-17,00

"LE ANALISI DEI RISCHI NEL GDPR"

A differenza della DPIA (art. 35) che deve essere eseguita solo nei casi espressamente previsti dalla normativa o quando si è in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche, le analisi dei rischi previste dagli artt. 24, 25 e 32 del GDPR sono sempre obbligatorie, per lo più disattese, e non riguardano solo aspetti di sicurezza.

Vi è quindi una diffusa incoerenza fra quanto richiesto dalla normativa e quando effettivamente agito. Se da un lato questo si traduce in una estesa mancanza di conformità da parte dei Titolari, dall'altro risultano carenti le adeguate misure tecniche ed organizzative poste a tutela delle persone fisiche ed il loro diritti.

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

Il relatore: Giancarlo Butti

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

GOOGLE CHROME SECURITY UPDATE FIXES 'HIGH RISK' FLAWS

22 luglio 2022 – Google has released security updates for Google Chrome browser for Windows, Mac and Linux, addressing vulnerabilities that could allow a remote attacker to take control of systems. *There are 11 fixes in total*, including five that are classed as high-severity. As a result, *CISA has issued an alert* encouraging IT administrators and regular users to install the updates as soon as possible to ensure their systems are not vulnerable to the flaws.
(source: https://www.zdnet.com/article/google-chrome-security-update-fixes-high-risk-flaws/)

LA CYBERSECURITY È ESG: COSA STA FACENDO FORTINET

22 luglio 2022 – Sempre più aziende stanno iniziando a condividere con i propri stakeholder i dati sui progressi ***ESG*** compiuti.

È questo il caso di **Fortinet**, azienda **californiana** del settore della **cybersecurity**. Scoperto l'interesse per queste tematiche, l'azienda si propone di condividere su base **annua** i propri progressi e successi.
E per farlo ha rilasciato il proprio primo **Sustainability Report**. Per riuscire ad avere un impatto positivo, l'azienda ha deciso di concentrarsi su **quattro** obiettivi principali: **innovare**, per rendere internet un luogo più sicuro; **rispettare l'ambiente**; creare un team di lavoro **inclusivo**, così da adempiere ai propri obiettivi in ambito sociale; e promuovere infine un business **responsabile**.
(source: https://www.money.it/la-cybersecurity-e-esg-cosa-sta-facendo-fortinet)

RANSOMWARE IN CRESCITA DEL 30%, PMI BERSAGLIO PREFERITO DEGLI HACKER

22 luglio 2022 – resce il numero delle imprese vittime di

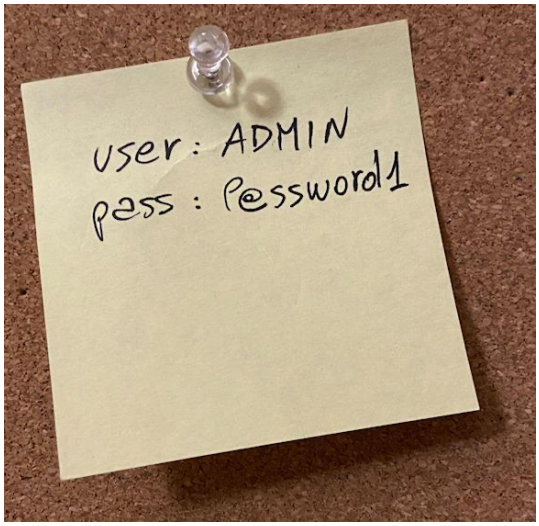
ISACA Roma (P.IVA: 11345311002 - C.F.: 97274880588) è un'associazione senza fini di lucro con sede in Roma.

ransomware: sono 707 gli obiettivi attaccati in 62 Paesi nel secondo trimestre del 2022, con **l'Italia quarto paese** tra i più bersagliati nel mondo. Si tratta di un dato **in crescita** del 37% sul medesimo periodo del 2021 e del **30% sul trimestre precedente**, con un **incremento significativo delle piccole e medie imprese** coinvolte: il 72% delle aziende vittime di esfiltrazioni di dati accompagnate a richieste di riscatto hanno un fatturato inferiore ai 250 milioni di dollari.
(source: https://www.corrierecomunicazioni.it/cyber-security/ransomware-in-crescita-del-30-pmi-bersaglio-preferito-degli-hacker/)

TROPPO POCHI GLI ESPERTI DI CYBER SECURITY IN ITALIA

23 luglio 2022 – Sono circa 6.000 i professionisti della cyber security presenti oggi in Italia. Un numero ancora troppo basso: siamo al terzo posto al mondo per attacchi da ransomware.
(source: https://www.corrierenazionale.it/2022/07/23/troppo-pochi-gli-esperti-di-cyber-security-in-italia/)

INCREDIBILE PARADOSSO: LA COMMISSIONE EUROPEA CITATA PER VIOLAZIONE DEL GDPR SU UN SUO STESSO PORTALE



23 luglio 2022 – Tutti ormai abbiamo sentito parlare, nel bene o nel male, del **GDPR**, il regolamento dell'Unione Europea in materia di trattamento dei dati personali che, sebbene sia a volte una scocciatura, ha sicuramente migliorato la privacy dei cittadini.
È però appena successo un fatto che ha il sapore di un incredibile paradosso internettiano: **la Commissione Europea è stata citata da un cittadino tedesco**, proprio per **violazione del GDPR**, e su un suo stesso portale. A supportare la denuncia troviamo anche la *Europäische Gesellschaft für Datenschutz* (EuGD).
(source: https://www.hwupgrade.it/news/web/incredibile-paradosso-la-commissione-europea-citata-per-violazione-del-gdpr-su-un-suo-stesso-portale_108868.html)

L'AGENZIA DELLE ENTRATE HA SUBITO UN ATTACCO INFORMATICO CON RICHIESTA DI RISCATTO

25 luglio 2022 – L'**Agenzia delle entrate sarebbe stata colpita da un *attacco informatico*** lanciato da una nota banda di cyber criminali, di probabile provenienza russa, chiamata ***Lockbit***. Secondo quanto diffuso sul sito dell'organizzazione, l'attacco avrebbe sottratto circa **78 gigabite di dati**, tra cui documenti relativi a "*Scansioni, report finanziari e contratti*". I criminali hanno dato tempo alle autorità fino al 31 luglio per pagare il *riscatto* dei dati ed evitare la loro pubblicazione.
(source: https://www.wired.it/article/attacco-informatico-agenzia-delle-entrate/?utm_medium=social&utm_source=linkedin)

WINDOWS 11 IS GETTING A NEW SECURITY SETTING TO BLOCK RANSOMWARE ATTACKS

22 luglio 2022 – Microsoft is rolling out a new security default for Windows 11 that will go a long way to preventing ransomware attacks that begin with password-guessing attacks and compromised credentials.
The new account security default on account credentials should help thwart ransomware attacks that are initiated after using compromised credentials or brute-force password attacks to access remote desktop protocol (RDP) endpoints, which are often exposed on the internet.
(source: https://www.zdnet.com/article/windows-11-is-getting-a-new-security-setting-to-block-ransomware-attacks/)

PROTEGGERE L'ITALIA È LA PRIORITÀ

23 luglio 2022 – Secondo l'esperto Enrico Ferretti, è un tassello importante. Il banchiere ha usato il cuore anche per la cybersecurity. E come ultimo atto da presidente del Consiglio ha chiuso il cosiddetto perimetro cyber dell'Italia per proteggere gli asset nazionali da hacker e infiltrazioni esterne. Mario Draghi si è congedato così. Con un provvedimento che, come spiega a ItaliaOggi l'esperto di sicurezza informatica Enrico Ferretti, «è un grande passo avanti per la definizione delle regole da adottare in determinati ambiti pubblici e privati».
(source: https://www.italiaoggi.it/news/proteggere-l-italia-e-la-priorita-2571108)

GOOGLE HA LICENZIATO L'INGEGNERE CHE AVEVA DEFINITO LA SUA INTELLIGENZA ARTIFICIALE "SENZIENTE"

23 luglio 2022 – **Google, la controllata di Alphabet, ha licenziato Blake Lemoine, l'ingegnere che un mese fa era salito alla ribalta delle cronache per definito "senziente" LaMDA, l'Intelligenza Artificiale** sviluppata dal gigante di Mountain View.
Google, che dopo le sue dichiarazioni aveva messo in congedo Lemonie, lo ha definitivamente messo alla porta, **sostenendo che l'ingegnere ha violato le politiche aziendali e che le sue affermazioni su LaMDA sono "del tutto infondate".**
(source: https://it.finance.yahoo.com/notizie/google-licenziato-lingegnere-che-aveva-185626179.html)

CYBERSECURITY ERGONOMICA

23 luglio 2022 – Ho avuto spesso modo di valutare differenti approcci alla protezione informatica, in diversi ambiti. Molte volte l'impostazione era troppo superficiale, le politiche di sicurezza insufficienti quando non completamente assenti, e questo esponeva l'azienda ad un fortissimo rischio di compromissione. A mio parere, però, quasi altrettanto deleterio per la sicurezza globale è l'implementazione di policy "troppo" stringenti.
So che questo sembra essere un controsenso, forse provocatorio, ma vi prego di seguirmi nel ragionamento...
(source: https://www.difesaonline.it/evidenza/cyber/cybersecurity-ergonomica)

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 dell'IT governance. CSX sta aiutando a plasmare il futuro della sicurezza informatica.

INFORMAZIONI UTILI

Chi ha già frequentato un corso a pagamento presso ISACA Roma ha uno sconto del 10%. Aziende, grossi enti, PAL, PAC e Difesa possono richiedere i costi a loro riservati alla casella **corsi<at>isacaroma<dot>it**
Per ulteriori informazioni sui corsi inviare una mail all'indirizzo: **corsi<at>isacaroma<dot>it**

Info e Contatti

info@isacaroma.it

Via Berna, 25 - 00144 Roma

Social Media

http://www.isacaroma.it/

SAPIENZA
UNIVERSITÀ DI ROMA

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

GET CERTIFIED

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

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

ANCHE QUESTO ANNO LA NEWSLETTER DI ISACAROMA VA IN VACANZA.
CI RIVEDREMO A SETTEMBRE

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.