Osservatorio Nazionale Informatica Forense

SECUREBIZ 2024

Dal 10 al 11 Maggio a FIRENZE

Florence Visitor Center - Piazza della Stazione 4

Associazione Informatica Professionisti

securebiz.it

INCIDENTI INFORMATICI IN AZIENDA

Prevenzione, Mitigazione, Analisi, Gestione

PROGRAMMA

VENERDI 10 MAGGIO 2024

Ore 9.30

Welcome e registrazione

Ore 10.00

Apertura Lavori:
Dott.ssa Antonella Ficini Presidente AIP ITCS
Ing. Paolo Reale Presidente ONIF
Prof. Fabio Gadducci Università di Pisa
La recente legislazione europea sull'insegnamento dell'informatica
Ing. Enrico Bocci Associazione Laureati in Scienze dell'Informazione

---

Ore 10.30

Dott. Alessandro Fiorenzi (ONIF):
Indagini informatiche forensi e incident response in azienda con strumenti opensource: Velociraptor e AWX ansible

ABSTRACT

In Aziende con decine o centinaia di postazioni di lavoro, dispositivi mobile e server in cloud e on premises, la Digital Forensics e soprattutto l'approccio DFIR sono strumenti fondamentali per gestire in efficienza ed efficacia situazioni di incident handling come data breach o violazione dei sistemi, ma anche per la gestione di indagini e investigazioni informatiche aziendali per la tutela del patrimonio aziendale: proprietà intellettuale, protezione dati, dipendenti infedeli, furti di informazioni riservate.

Processi e strumenti della DF e della DFIR possono essere usati proficuamente anche per Audit di sicurezza in ambito ISO27001, Dlgs 231/01, GDPR, NIS II, DORA, etc.. garantendo la genuinità delle prove in quanto raccolte in modo "forense".

Velociraptor e AWX Ansible sono due strumenti OpenSource che si usano in ambito aziendale per eseguire indagini informatiche e raccogliere prove su larga scala con modalità forensi, ma anche e soprattutto per gestire incidenti di sicurezza e data breach in modo forense

BIO

Libero professionista da oltre 20 anni, Alessandro Fiorenzi si occupa professionalmente di Sicurezza informatica, compliance, auditing IT, e Informatica Forense a cui dedica il suo maggior impegno.

Con il patrocinio di:

Partner dell'evento:

In qualità di Consulente Informatico Forense per privati, aziende e Autorità Giudiziarie, ha maturato competenze significative in vari ambiti della digital forensics, dalla computer forensics, la mobile forensics e network forensics, dedicando particolare interesse e impegno alle indagini informatiche forensi in ambito aziendale, in particolare riguardo agli aspetti giuslavoristici, di webreputation, di tutela del patrimonio aziendale, e di contratti e servizi IT.

E' Iscritto all'albo dei CTU e dei Periti del Tribunale di Firenze, e all'Albo Periti ed Esperti CCIAA Firenze, è anche Consulente Arbitratore della stessa. Ha partecipato come CTU/CTP processi di rilevanza nazionale.

Abilitazione NATO NCAGE AT568, Certificato ECCE (European Certificate on the fight against Cybercrime and Electronic Evidence), Lead Auditor ISO 27001,Membro Pool of Expert of EDPB nelle specializzazioni "Technical expertise in new technologies and information security" e "Legal expertise in new technologies", membro del Comitato Scientifico CLUSIT dal 2012 al 2022, membro di ANRA Ass. Naz.le Risk Manager, iscritto all'Albo MISE Innovation Manager e membro del CDA di Security Broker.

Ha collaborato al libro "Internet e il danno alla persona" edito da Giappichelli nel 2012; è organizzatore e relatore di vari convegni sul tema della Digital Forensics.

E' laureato in Scienze dell'Informazione all'Università degli studi di Firenze nel 2001.

Ore 10:25

Avv. Filippo Bianchini (AIP):
Il regolamento DORA sulla resilienza operativa digitale

ABSTRACT

Abstract: Il Digital Operational Resilience Act, o DORA, è un regolamento dell'Unione Europea (UE) che stabilisce un framework vincolante e completo riguardante la gestione del rischio delle tecnologie di informazione e comunicazione per il settore finanziario dell'UE. Il regolamento DORA stabilisce gli standard tecnici che le entità finanziarie e i loro fornitori critici di servizi tecnologici di terze parti devono implementare nei propri sistemi ICT entro il 17 gennaio 2025.

BIO

L'Avv. Filippo Bianchini, abilitato al patrocinio innanzi alle Giurisdizioni Superiori, si è laureato in Giurisprudenza presso l'Università degli Studi di Perugia; nel 2006 ha fondato lo Studio Legale Bianchini e svolge attività principalmente nei settori data protection & privacy, diritto dell'IT e diritto civile; si interessa, tra l'altro, di computer forensics e del contrasto ai fenomeni di cyberstalking e cyberbullismo. È un mediatore professionista.

Si occupa di gestione della sicurezza delle informazioni e della protezione dei dati personali e svolge attività di adeguamento al Regolamento (UE) 2016/679, di Data Protection Officer (certificato UNI 11697:2017) e di auditing (certificato Auditor/Lead Auditor di Sistemi di gestione della sicurezza delle informazioni - UNI CEI ISO/IEC 27001:2013 e Valutatore privacy UNI 11697:2017).

Contemporaneamente all'attività professionale, ha frequentato corsi avanzati di diritto sostanziale e processuale dell'Unione Europea; è docente di informatica giuridica per la Scuola Forense "G. Gatti" dell'Ordine degli Avvocati di Perugia e docente del Master universitario in "Data protection, Cybersecurity e Digital forensics" dell'Università per gli Studi di Perugia; è, inoltre, relatore in numerosi convegni in materia di data protection e cyber security.

È membro del Cyber Security National Lab, nodo di Perugia, e dell'Internet of Things Council, nonché socio del Circolo Giuristi Telematici e dell'Associazione Informatici Professionisti.Segue l'evoluzione dei fenomeni legati ad internet ed alle nuove tecnologie, con particolare attenzione a legal tech, intelligenza artificiale e blockchain.

Con il patrocinio di:
Partner dell'evento:

Ore 10:50

Prof. Rocco De Nicola (IMT):

Skill shortage: la formazione Universitaria vs. le esigenze delle imprese nell'area della Cybersecurity

ABSTRACT

...

BIO

E' professore ordinario di Informatica presso la Scuola IMT Alti Studi Lucca e collabora con il Gran Sasso Science Institute (GSSI) dell'Aquila dove ha coordinato per i primi quattro anni il programma di dottorato in Informatica. Alla Scuola IMT De Nicola dirige l'unità di ricerca SySMA e coordina il programma di dottorato in Systems Science.

E' stato professore ordinario anche all'Università di Firenze e alla Sapienza Università di Roma. In precedenza è stato ricercatore al CNR di Pisa e ha lavorato prima all'Università di Edimburgo, poi per Italtel a Milano e alla Olivetti di Pisa. È stato visiting professor all'École Normale Supérieure di Parigi e all'Università Ludwig Maximilian di Monaco, e visiting scholar alla Microsoft Research di Cambridge. Ha conseguito la laurea in Scienze dell'informazione all'Università di Pisa nel 1978 e ha ricevuto un dottorato di ricerca in Informatica dall'università di Edimburgo nel 1985.

Ore 11:20

Prof. Michele Ferrazzano (ONIF):

La selezione dei dati informatici in ambito giudiziario tra prassi operative, giurisprudenza, novità normative e strategia processuale

ABSTRACT

In ambito di digital forensics, sotto un profilo strettamente tecnico, la copia forense è sempre stata considerata l'operazione principe che distingue l'intervento dell'esperto rispetto a un "generico" informatico. Ciò in ragione del fatto che, alla fine dell'accertamento, ogni parte avrebbe la possibilità di verificare il lavoro a partire proprio dalla copia forense.

Tuttavia, la giurisprudenza e le norme che via via vengono introdotte, rivedono tale procedimento in un'ottica di maggior tutela del diritto alla riservatezza del singolo e del patrimonio informativo aziendale.

In questo quadro, verrà rappresentato in che modo potrebbe essere proposto un accertamento tecnico anche mediante un significativo uso di soluzioni di data room per la selezione delle sole evidenze rilevanti, comprimendo il periodo di intervento dell'esperto di informatica forense e degli altri professionisti coinvolti nell'individuazione dei dati pertinenti (avvocati e consulenti tecnici esperti di altre materie) e dandogli un ruolo cruciale rispetto all'esito del procedimento giudiziario in fatto di individuazione delle evidenze informatiche.

Con il patrocinio di:
Partner dell'evento:

BIO

Socio fondatore ONIF, Michele Ferrazzano E socio di BIT4LAW, azienda di consulenza informatica forense con sede a Bologna, Milano, Roma e Siracusa che offre servizi di laboratorio e consulenza tecnica informatica forense, sicurezza informatica, incident response, privacy e gestione data breach.

Laureato in informatica all'Università di Bologna, ha conseguito un dottorato in Diritto e Nuove Tecnologie presso il CIRSFID Università di Bologna.

Ha ricoperto numerosi incarici accademici, attualmente E professore a contratto di Computer forensics all'Università di Milano e professore a contratto di Informatica all'Università di Modena e Reggio Emilia.

Ore 11:50

Dott. Pier Luca Toselli (GdF):

L'importanza della digital forensics nelle imprese. Come gestire correttamente un incidente e saperlo segnalare alle autorità. Qualche tool e tecnica di aiuto.

ABSTRACT

Evidenzierò l'importanza della digital forensics fin dalle prime fasi dell'incidente informatico, un focus che faccia comprendere all'azienda l'importanza di saper "congelare" e "segnalare" ciò che è utile per l'avvio di una indagine da parte delle autorità. Qualche esempio su concorrenza sleale frodi da parte di aziende sul WEB, come segnlare un "insider" infedele e altro. Spunti pratici con anche l'utilizzo di uno /due tool.

BIO

Ufficiale di polizia giudiziaria in servizio attivo nella Guardia di Finanza, ha maturato un'affinata e documentata esperienza nel settore delle investigazioni di polizia giudiziaria ed economico-finanziaria, con specifico riferimento alla Digital Forensics, per la quale ha anche conseguito la qualifica di Computer Forensics e Data Analysis. L'esperienza ultratrentennale gli ha permesso di conseguire anche una solida preparazione tecnico-giuridica, documentata da certificazioni, diversi corsi di alta formazione universitaria e dal Perfezionamento in Criminalità Informatica e Investigazioni Digitali presso l'Università di Milano. È stato docente nell'ambito del Master Executive di II livello in Criminologia e cyber Security (Master Sida - Fondazione INUIT Tor Vergata) e formatore FIRST RESPONDER per la Guardia di Finanza. Relatore in diversi convegni di settore è anche autore di articoli tecnico giuridici dedicati alla Digital Forensics su diverse riviste e di recente sul MEMBERBOOK IISFA. Socio IISFA, ONIF e OSINTITALIA.

Ore 12:20

Ing. Anna Vaccarelli (CNR):

Cybersecurity nelle aziende: nuovi scenari

ABSTRACT

Fino a pochi anni fa la cybersecurity nelle aziende non era un tema attuale, sembrava riguardare solo le aziende IT. Oggi lo scenario è cambiato: gli attacchi sono in costante aumento ed è evidente che il problema non riguardi solo le aziende IT, ma

Con il patrocinio di:
Partner dell'evento:

quelle manifatturiere, dei trasporti e logistica, la sanità con tutte le loro filiere. Diventa, quindi, necessario dotarsi di personale e di strumenti tecnici adeguati: la figura del CISO è centrale e deve avere accesso diretto ai vertici aziendali e il team di cybersecurity è strategico per ogni azienda, che sia interno o esterno. L'attenzione alla cybersecurity diventa urgente soprattutto oggi che l'intelligenza artificiale sta aprendo nuove sfide sia negli scenari di attacco che in quelli di difesa

BIO

laureata all'Università di Pisa in Ingegneria elettronica. Dal 2004 è responsabile delle relazioni esterne del Registro.it, l'anagrafee dei domini.it, gestito dallo Istituto di Informatica e Telematica del Cnr. Dal 2010 coordina e promuove un'azione di diffusione della cultura di internet nelle scuole. È tra i fondatori di Internet Festival e fa tutt'ora parte del comitato scientifico. E' sua anche la trasmissione radiofonica di divulgazione scientifica "Aula40"

Ore 12:45

Pausa buffet

Ore 13:40

Massimo Chirivì (AIP/AIPSI):
Quali sono i rischi se non si conosce il perimetro dell'azienda e la superficie di attacco?

ABSTRACT

In tantissime circostanze noi esperti di Sicurezza Informatica, ci ritroviamo ad osservare che l'azienda non conosce cosa difendere e dove è collocato l'asset da mettere in protezione, non si rende conto dei rischi collegati ad avere ad esempio un account linkedin aziendale, o banalmente la PEC su un fornitore cloud qualsiasi.

Il perimetro dell'azienda è diventato da molti anni un perimetro virtuale che va individuato e gestito correttamente, come anche la superficie di attacco che è variata negli anni, gli oggetti connessi sono aumentati esponenzialmente e di conseguenza sono aumentati anche i rischi connessi.

In questo intervento si affronterà la situazione attuale comprendendo meglio come affrontare le sfide odierne

BIO

Massimo Chirivì, nasce nel 1976 e vive in provincia di Lecce, è una figura poliedrica nel panorama dell'ICT, ricoprendo ruoli di Ethical Hacker, IT Security Expert, System Engineer, Web Designer e ICT Consultant. Dopo aver conseguito la maturità tecnica industriale nel 1996, ha intrapreso un percorso di formazione continua che lo ha portato ad essere un punto di riferimento nel settore. Fondatore e CEO di Innovamind srls, è noto per il suo impegno nello sviluppo di soluzioni di sicurezza informatica e nella ricerca, collaborando con partner di rilievo come Microsoft e DELL. La sua carriera è costellata da oltre 100 seminari, workshop e partecipazioni a eventi nazionali ed internazionali, dimostrando un impegno costante all'aggiornamento e alla condivisione delle sue conoscenze. Docente di ICT Security & Ethical Hacking e DPO, Chirivì ha anche una lunga esperienza come consulente per importanti enti e aziende, affrontando sfide nel campo della sicurezza delle informazioni e dello sviluppo tecnologico. La sua visione e competenza nell'ICT lo rendono un relatore d'eccezione, capace di offrire spunti di riflessione e soluzioni innovative per affrontare le sfide del digitale.

Con il patrocinio di:

Partner dell'evento:

Ore 14:10

Dott. Cosimo de Pinto (AIP/ONIF):
Gestire la Cyber Response: eventi, compromissioni e monitoraggio. Come fare?

ABSTRACT

Gli incidenti di sicurezza informatica possono avere un impatto devastante sulle aziende, specie in ambito Corporate, e possono causare gravi danni organizzativi e finanziari oltre quelli inerenti l'immagine e la cosiddetta Web Reputation. È indispensabile disporre di processi e procedure efficaci per affrontarli in modo rapido ed efficiente, al fine di ridurre al minimo l'impatto. Uno dei fattori fondamentali per una corretta gestione è sicuramente il tempo di risposta.

Oggi vi sono strumenti di verifica dei sistemi coinvolti in grado di dare risposte pressoché immediate in ambiente live e post-mortem: l'integrazione di THOR con Velociraptor si propone di potenziare la Digital Forensics e l'Incident Response.

VELOCIRAPTOR è uno strumento DFIR gratuito e open source unico nel suo genere, che offre potenza e flessibilità grazie al Velociraptor Query Language che consente la ricerca e il recupero di un tipo specifico di informazioni da un endpoint, semplificando così le attività forensi e di monitoraggio.

THOR è uno strumento avanzato di valutazione delle compromissioni, progettato e sviluppato per rilevare strumenti di hacking, backdoor e tracce di attività malevoli sugli endpoint in esame; è in grado di esaminare i sistemi alla ricerca di segni di strumenti di attacco, manipolazioni del sistema e attività di registro sospette.

Considerando il classico scenario in cui si nota un'attività di rete insolita proveniente da un host all'interno della rete aziendale, da dove cominciare?

Il talk affronterà il tema della Cyber Response proponendo una panoramica degli strumenti open source idonei a gestire e monitorare gli eventi degli endpoint.

BIO

Laureato in Beni Culturali, è stato un pioniere della Digital Forensics, espletando il suo primo incarico quale ausiliario di P.G. nel lontano 1990, presso la Procura di Bari. Con oltre 34 anni di esperienza in Digitals Forensics, si occupa anche di Cyber Security dal 2002. Certificato CIFI (Certified Information Forensics Investigator), membro ONIF (Osservatorio Nazionale per l'Informatica Forense), membro IISFA (International Information System Forensics Association), membro AIP (Associazione Informatici Professionisti), è iscritto all'Albo dei Periti e C.T. presso il Tribunale di Roma e opera come Consulente Tecnico di Parte, Ausiliario di Polizia Giudiziaria - in attività di sequestro e perquisizione - e Consulente Tecnico di Ufficio per l'Autorità Giudiziaria. Ha ricoperto numerosi incarichi come C.T. e perito sia in ambito penale che civile, oltre che per indagini preventive e incarichi stragiudiziali.

É stato docente al master di Criminologia presso l'Istituto Nazionale di Pedagogia Familiare e presso la Scuola Internazionale di Polizia di Caserta.

Titolare di uno studio professionale a Roma, presta la propria consulenza a studi legali, aziende, privati, Procure e FF.OO., in materia di Digital Forensics e Cyber Crime. Relatore in vari convegni sul tema della Digital Forensics, l'ultimo nel 2023, alla Cyber Crime Conference tenutosi a Roma nel maggio 2023 con un talk sul tema dell'Anti-Forensics.

Pubblica come autore su ICT Security Magazine articoli tecnici sul mondo della Digital Forensics.

Con il patrocinio di:
REGIONE TOSCANA
CONFASSOCIAZIONI Digital
Clusit
Camera di Commercio Firenze dal 1770 la casa delle imprese
Università di Pisa
Partner dell'evento:
EDP YOUR INFORMATION TECHNOLOGY PARTNER
DARKBOX CYBERSECURITY
RICOH imagine. change.

Ore 14:35

Avv. Federica De Stefani:
L'incidente informatico: responsabilità, contratti e figure coinvolte

ABSTRACT

Un contratto può regolare la gestione di un incidente informatico? Allo stesso modo un contratto può determinare la responsabilità delle figure coinvolte nelle attività immediatamente successive all'incidente? E in quelle antecedenti all'incidente stesso? In questo intervento risponderemo a questi interrogativi e valuteremo come si costruisce (e si sottoscrive) un contratto che garantisca una tutela effettiva sia dell'azienda, sia dei professionisti coinvolti.

BIO

Avvocato, iscritta all'ordine degli Avvocati di Mantova, con competenze specifiche in materia diritto delle nuove tecnologie, privacy, contrattualistica e diritto sportivo. Professore a contratto di Link Campus University e Unicollege SSML, collabora con diverse Università italiane Collabora con il Centro di ricerca DITES della Link Campus University e con la rivisita del Centro "Quanderni di comunità". Maestro della Protezione dei dati & Data Protection; Designer; DPO .
Perfezionata in: Data Protection e Data Goverance, Big data, Intelligenza artificiale e piattaforme, Criminalità informatica e investigazioni digitali, Legal tech

Ore 15:05

Prof. Ing. Ugo Lopez (ONIF/AIP):
Data protection per aziende e studi professionali: approccio essenziale per la sicurezza di dati e informazioni

ABSTRACT

Nell'era digitale, la sicurezza informatica e l'analisi forense digitale rappresentano due pilastri fondamentali per la protezione delle informazioni e la risposta agli incidenti informatici. L'intervento mira a esplorare l'intersezione tra queste due discipline e a dimostrare come la loro integrazione possa offrire una strategia di difesa più robusta contro le minacce informatiche. Attraverso l'analisi delle migliori pratiche, si evidenzierà come la forensic readiness, ovvero la preparazione all'analisi forense, possa migliorare la capacità di un'organizzazione di prevenire, rilevare e rispondere efficacemente agli attacchi informatici. Verranno inoltre discusse le sfide legate all'integrazione di queste discipline, come la necessità di formazione specifica per gli esperti di sicurezza e la gestione della privacy e della protezione dei dati nel contesto delle indagini digitali. L'obiettivo è quello di fornire una panoramica completa su come un approccio integrato alla cybersecurity e alla digital forensics possa non solo migliorare la sicurezza informatica ma anche accelerare il processo di indagine e risposta agli incidenti, contribuendo così alla creazione di un ambiente digitale più sicuro e resiliente. Questo intervento sottolinea l'importanza di un approccio olistico alla sicurezza informatica, mettendo in luce come l'integrazione tra cybersecurity e digital forensics possa portare benefici tangibili alle organizzazioni nell'ambito della prevenzione, rilevamento e risposta agli incidenti informatici.

BIO

Professore straordinario di Informatica Forense nel corso di Laurea Magistrale in Sicurezza Informatica presso UniBA, Ingegnere informatico e giurista attivo da molti anni nel settore della Digital Forensics, ha svolto svariate consulenze di parte e perizie giurate. Socio Ordinario ONIF, opera dal suo studio di Bari.

Con il patrocinio di:
REGIONE TOSCANA
CONFASSOCIAZIONI Digital
Clusit
Camera di Commercio Firenze dal 1770 la casa delle imprese
UNIVERSITÀ DI PISA
Partner dell'evento:
EDP YOUR INFORMATION TECHNOLOGY PARTNER
DARKBOX CYBERSECURITY
RICOH imagine. change.

Ore 15:35

Dott. Claudio Telmon (CLUSIT):
NIS2, DORA,CRA...: approccio integrato alla conformità alle nuove norme sulla cybersecurity

ABSTRACT

La gestione della cybersecurity in azienda nei prossimi anni sarà caratterizzata dall'esigenza di garantire la conformità ad un gran numero di norme specifiche, europee e nazionali. Individuare a quali norme un'azienda si debba adeguare, in quali tempi, ed affrontarle in modo integrato sarà un'esigenza per riuscire a tenere sotto controllo la proliferazione di attività e di requisiti da gestire. D'altra parte, le norme europee recentemente emanate o in corso di emanazione rappresentano un framework coordinato, di cui è utile capire le logiche per rendere più efficienti le azioni di adeguamento. L'intervento parte dalle principali norme di riferimento, per individuare i punti di contatto e le attività che possono essere affrontate in modo integrato nei diversi ambiti.

BIO

Claudio Telmon è consulente e adviser nel campo della sicurezza e dell'audit ICT, comprendendo aspetti di gestione e configurazione dei sistemi, lo sviluppo di software, la progettazione e implementazione di ISMS, la formazione, la ricerca, fino alle problematiche ICT relative alla Business Continuity. Ha studiato presso l'Università di Pisa, dove ha ottenuto una laurea in Laurea in Scienze dell'Informazione. Dal 2009 al 2011 è stato docente a contratto di "Metodi e Strumenti per la sicurezza" per la Laurea Magistrale in Sicurezza Informatica presso l'Università di Pisa, polo di La Spezia e dal 2010 al 2011 è stato docente a contratto di "Crittografia avanzata" per la Laurea Magistrale in Sicurezza Informatica sempre presso l'Università di Pisa, polo di La Spezia. È stato Socio Fondatore e Membro del Comitato Direttivo di AIPSI Associazione Italiana Professionisti della Sicurezza Informatica. Dal 2002 è Membro del Comitato Direttivo di CLUSIT, Associazione Italiana per la Sicurezza Informatica.

Ore 16:05

Dott. Davide De Luca
I rischi privacy nella gestione del personale alla luce dei maggiori controlli della Cybersecurity con l'intelligenza artificiale

ABSTRACT

In un contesto caratterizzato da una crescente digitalizzazione dei processi aziendali, l'impiego dell'intelligenza artificiale (IA) rappresenta una svolta significativa per la sicurezza informatica e la gestione del personale. Questo intervento si propone di esplorare il complesso equilibrio tra la necessità di proteggere i dati personali dei dipendenti e l'implementazione di soluzioni di cybersecurity basate sull'IA, in un panorama normativo in evoluzione. Con l'annuncio del recente accordo politico del Consiglio Europeo su un disegno di legge per un'IA sicura, rispettosa dei diritti fondamentali e promotrice della prosperità aziendale, diventa imperativo analizzare le implicazioni per la privacy e i rischi associati all'uso dell'IA nella gestione del personale.

Attraverso l'analisi di casi di studio e un'esame approfondito della legislazione, incluso il GDPR, verranno evidenziati i rischi per la privacy derivanti dall'uso dell'IA in ambito di sorveglianza dei dipendenti, elaborazione automatica dei dati e decisioni algoritmiche. Queste tecnologie, sebbene promettenti per l'efficienza aziendale e la prevenzione delle minacce informatiche, sollevano questioni etiche e legali significative riguardo al consenso, alla trasparenza, alla non discriminazione e al diritto alla spiegazione.

Con il patrocinio di:
Partner dell'evento:

Particolare enfasi sarà posta sull'interpretazione del nuovo quadro legislativo europeo sull'IA, esaminando come le aziende possono adeguarsi alle normative garantendo al contempo l'innovazione e la sicurezza. Verranno discusse le best practices per integrare l'IA nella cybersecurity e nella gestione del personale in modo etico e conforme, come l'adozione di principi di accountability, la minimizzazione dei dati e la valutazione d'impatto sull'IA, parallela alla DPIA, che consideri specificamente i rischi per i diritti e le libertà individuali legati all'uso dell'IA. Il dibattito si amplierà quindi alle strategie proattive per mitigare i rischi privacy nell'uso dell'IA, enfatizzando l'importanza di un approccio partecipativo nella progettazione e implementazione delle tecnologie di IA, coinvolgendo stakeholder interni ed esterni per assicurare che i sistemi di IA siano non solo tecnicamente avanzati, ma anche eticamente responsabili e socialmente accettabili.

L'obiettivo dell'intervento è di offrire una panoramica critica sui rischi e sulle opportunità presentati dall'integrazione dell'IA nella gestione della cybersecurity e del personale, alla luce del nuovo disegno di legge europeo sull'IA. Si intende fornire ai responsabili ICT aziendali (CIO/CTO) e al management nei settori legal/HR, gli strumenti necessari per navigare le sfide poste dall'IA, promuovendo una cultura aziendale che consideri la sicurezza informatica e la privacy dei dipendenti come pilastri di un'innovazione responsabile e sostenibile nel futuro digitale.

BIO

Informatico forense esperto in cybersecurity e telecomunicazioni. Consulente del Tribunale di Catania e delle Forze dell'Ordine. Laureato con lode all'Università di Teramo con tesi in ICT per le organizzazioni. DPO certificato UNI11697, svolge la professione presso diversi enti pubblici e privati. docente in Master Universitari per Data Protection e Cybersecurity con specializzazione in sanità e ricerca scientifica. Auditor ISO27001 con est. ISO27701, ISO37001 e ISDP10003.

Ore 16:35

Dott. Andrea Lazzarotto (ONIF):
Ottenere risposte immediate dall'analisi dei file di log con SQLite

ABSTRACT

Gli accertamenti tecnici relativi ad accessi abusivi e furti di dati informatici richiedono spesso l'analisi di grandi quantitativi di log, con migliaia di righe dalle quali è necessario riconoscere elementi ricorrenti e isolare le anomalie. Si rivela altresì importante correlare e incrociare log provenienti da fonti diverse.

L'intervento ha lo scopo di mostrare come utilizzare SQLite per l'analisi dei log e ottenere risposte in modo rapido ed efficace. Si tratta di uno strumento apparentemente semplice, ma molto potente che consente di ridurre il tempo necessario per ricostruire ciò che è avvenuto. Verranno mostrati due esempi pratici relativi ad accessi abusivi a sistemi informatici.

BIO

Socio ordinario ONIF, Andrea Lazzarotto ha conseguito la laurea magistrale con lode in Informatica, con una tesi dedicata alla ricostruzione forense di file-system NTFS con metadati danneggiati. Opera da anni come consulente informatico forense e parallelamente ha maturato una profonda esperienza nel campo delle applicazioni mobili, sia dal punto di vista realizzativo (sviluppo software) che dal punto di vista di analisi di funzionamento e di sicurezza (reverse engineering), in particolar modo su piattaforma Android.

Nell'attività professionale si dedica anche all'approfondimento dell'anti-forensics. In particolare, ha condotto ricerche approfondite sulla documentazione dei metodi per manomettere le chat di WhatsApp, al fine di delineare metodologie per verificarne la genuinità e l'integrità.

Con il patrocinio di:
REGIONE TOSCANA
CONFASSOCIAZIONI Digital
Clusit
Camera di Commercio Firenze dal 1770 la casa delle imprese
Università di Pisa
Partner dell'evento:
EDP YOUR INFORMATION TECHNOLOGY PARTNER
DARKBOX CYBERSECURITY
RICOH imagine. change.

Oltre ad alcune attività di docenza nel settore, ha contribuito allo sviluppo di tecniche di acquisizione forense di contenuti web, come ad esempio la cristallizzazione di profili Instagram tramite API.

È autore di RecuperaBit, un software open source per l'analisi forense di partizioni NTFS e Carbon14, uno strumento dedicato alla datazione delle pagine web. Ha contribuito allo sviluppo di CAINE, distribuzione Linux per la digital forensics. È inoltre un componente del team di FIT, un innovativo programma di acquisizione forense di pagine web.

Ore 17:00

Alessio L.R. (mayhem) Pennasilico (AIP/Clusit)

Quanto la Cyber Security può impattare i temi ESG?
Environment, sustainability, governance

ABSTRACT

Quando pensiamo alla sostenibilità pensiamo quasi esclusivamente alla tutela dell'ambiente e all'inclusività. Per quanto questi pillar siano fondamentali va ricordato il fine ultimo dei sistemi ESG ovvero la tutela degli stakeholder, tutti, nonché garantire fiducia e affidabilità al mercato. Vedremo quindi come la cybersecurity possa impattare positivamente sul rating ESG e più in generale sulla percezione che il mercato ha dell'azienda.

BIO

Information & Cyber Security Advisor, Security Evangelist, noto nell'hacker underground come - mayhem -, è internazionalmente riconosciuto come esperto dei temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie. Per questa ragione partecipa da anni come relatore ai più rilevanti eventi di security italiani ed internazionali ed è stato intervistato dalle più prestigiose testate giornalistiche, radio e televisioni nazionali ed internazionali.

All'interno di P4I, per importanti Clienti operanti nei più diversi settori di attività, sviluppa progetti mirati alla riduzione dell'impatto del rischio informatico/cyber sul business aziendale, tenendo conto di compliance a norme e standard, della gestione del cambiamento nell'introduzione di nuovi processi ed eventuali tecnologie correlate.

Credendo che il cyber risk sia un problema organizzativo e non un mero problema tecnologico, Alessio da anni aiuta il top management, lo staff tecnico e l'organizzazione nel suo complesso a sviluppare la corretta sensibilità in merito al problema, tramite sessioni di awareness, formazione e coaching.

Alessio è inoltre membro del Comitato Direttivo e del Comitato Tecnico Scientifico di Clusit, Già presidente di Associazione informatici Professionisti - AIP, membro del Comitato di Schema UNI 11506 di Kiwa Cermet e Vice Presidente del Comitato di Salvaguardia per l'Imparzialità di LRQA, l'ente di certificazione dei Lloyd's.

Ore 20:30

Cena sociale AIP-ITCS e ONIF

Con il patrocinio di:
Partner dell'evento:

SABATO 11 MAGGIO 2024

Ore 9:30

Dott. Marco Marcellini:
Hacking e pentesting ai tempi dell'IA

ABSTRACT

Gli immensi progressi nel campo dell'intelligenza artificiale (AI) stanno avendo un ampio impatto nel settore della sicurezza informatica, sia dal lato degli attaccanti che dei difensori. L'IA mette a disposizione, senza particolari barriere all'entrata, sofisticate tecniche di attacco e nuovi modelli per aumentare l'efficienza dei metodi di attacco già noti. L'intervento intende mostrare come sia possibile, in pochi semplici passi, utilizzare l'IA per ottenere rapidamente informazioni su un possibile obiettivo o come rintracciare vulnerabilità in applicazioni web grazie a codice AI-driven.

BIO

Marco Marcellini si occupa dal 1995 di nuove tecnologie e ha partecipato a numerosi progetti che hanno Internet come protagonista; tra le collaborazioni più importanti quella con Lorenzo Cherubini (Jovanotti) che ha scritto di lui come "uno dei migliori esperti di cultura digitale e di rete in circolazione". Laurea in economia, Master in cyber security, e' criminologo, esperto in scienze forensi ed hacker etico. Consulente presso Procure e Tribunali, si occupa di formazione e divulgazione della sicurezza in Rete

---

Ore 10:00

Paolo Giardini (AIP):
Threat intelligence

ABSTRACT

Nel panorama digitale attuale, le minacce cyber diventano sempre più sofisticate e frequenti. Le organizzazioni devono rimanere proattive nelle loro misure di sicurezza per proteggere i loro dati e le loro risorse di valore. La Threat Intelligernce svolge un ruolo critico in questo contesto, fornendo informazioni sulle potenziali minacce cyber, le loro fonti e come mitigarle. In questo intervento, introdurremo il concetto di Threat Intelligence e discuteremo della sua importanza nella cybersecurity moderna.

BIO

Paolo Giardini si occupa da oltre 25 anni di audit, analisi e consulenza nelle materie relative alla Sicurezza Informatica, Privacy e Data Protection, Digital Forensics, Computer and Networks Forensics, consulenza di direzione in merito alla gestione e protezione delle informazioni. Ha inoltre partecipato al gruppo di lavoro sul Codice di autoregolamentazione per Internet Service Provider promosso dal Garante Privacy. Consulente per la Comunità Europea nel progetto ENCYSEC Enhancyng Cyber Security è membro del Roaster of Expert di ITU International Telecommunication Union dell'ONU e del FORMEZ, Centro Studi e Formazione della PA. Presta consulenze come Consulente Tecnico di parte e Consulente Tecnico d'Ufficio in Digital Forensics per Procure della Repubblica e privati. Ha effettuato docenze per i corsi di Computer Forensics e di Comunicazioni Digitali dell'Università di Perugia e del corso OSINT nel Master di Intelligence Economica presso l'Università di Tor Vergata. Tiene corsi su sicurezza informatica, digital forensics, privacy, investigazioni digitali, OSINT, cyberbullismo, consapevolezza e sicurezza online presso università, pubbliche amministrazioni, forze di polizia, scuole. E' in possesso della qualifica come Lead Auditor ISO/IEC 27001:2017, ISO/IEC 27001:2022 e ISO/IEC 27701:2019. E' certificato EUCIP (European Certification of Informatics Professionals). E' inoltre stato qualificato come Lead Auditor per lo schema Data Privacy Certification GDPR di Bureau Veritas.

Con il patrocinio di:
REGIONE TOSCANA
CONFASSOCIAZIONI Digital
Clusit
Camera di Commercio Firenze dal 1770 la casa delle imprese
Università di Pisa
Partner dell'evento:
EDP YOUR INFORMATION TECHNOLOGY PARTNER
DARKBOX CYBERSECURITY
RICOH imagine. change.

Ore 10:30

Dott. Fabio Terrone (ONIF/AIP):
Managed detection & response: DF, AI e cybersec

ABSTRACT

Illustrazione del ruolo cruciale del Managed Detection and Response (MDR) in sinergia con l'Intelligenza Artificiale (AI), il Machine Learning (ML) e la Digital Forensics. L'AI e il ML, attraverso l'analisi predittiva e la rilevazione basata su comportamenti anomali, migliorano la capacità del MDR nella prevenzione e risposta alle minacce in tempo reale. Esempi di come la Digital Forensics contribuisce alla comprensione approfondita delle violazioni, facilitando la ricostruzione degli eventi e il miglioramento continuo della Cybersecurity. Infine alcune raccomandazioni per implementare una strategia efficace di Digital Forensics, basata sull'effettiva collaborazione tra le diverse funzioni aziendali, gli esperti del settore e le autorità competenti.

BIO

Socio ordinario ONIF, Fabio Terrone svolge l'attività di consulente informatico forense sin dal 2001 collaborando con diverse Procure del Lazio e con quella di Milano come consulente tecnico del PM, anche con la Direzione Distrettuale Antimafia di Roma; con il Tribunale Penale di Velletri e Frosinone come perito del Giudice; con la Polizia Giudiziaria come ausiliario di PG; con il Tribunale Civile di Roma come C.T.U del Giudice; con le parti civili (Aziende, Privati) come Consulente Tecnico di Parte. L'esperienza lavorativa pregressa in una multinazionale americana e la creazione e gestione di una propria azienda nel settore della sicurezza informatica, completano le diverse competenze acquisite nel tempo e da perseguire sempre.

Ore 11:00

Ing. Enrico Tonello (AIP):
Attacchi di cifratura e Business Continuity

ABSTRACT

La comunicazione verterà sull'illustrazione di cosa sia un attacco Ransomware di cifratura e quali canali vengano comunemente utilizzati per infiltrarsi sulle macchine (PC e Server) e per poi cifrare i dati. Al termine di questa prima parte preliminare si procederà ad illustrare alcune delle tecnologie che sono da considerarsi tra le più efficaci ed efficienti, allo stato attuale dell'arte, per bloccare la cifratura nella fase iniziale dell'attacco e rendere minimi i danni da questa provocati e quale tecniche di ripristino e di rimessa in produzione delle macchine. Al completamento di questa necessaria illustrazione si procederà ad effettuare un attacco Ransomware recente attivato in modalità HUMAN OPERATED RANSOMWARE ATTACK su una macchina virtuale totalmente isolata per mostrare cosa accada e come ma anche, e soprattutto, gli effetti devastanti che questo produce e la durata di un attacco di cifratura senza sistemi di protezione specifici.Poi a conclusione si procederà ad effettuare il medesimo attacco Ransomware sempre attivato in modalità HUMAN OPERATED RANSOMWARE ATTACK sulla stessa macchina virtuale totalmente isolata ma con sistema di protezione attivo per mostrare come il processo di cifratura venga controllato nella sua fase iniziale e gli effetti molto limitati che questo produce ove i file sono recuperabili nell'ordine di 5/10 minuti e la macchina possa ritornare praticamente nell'immediatezza in produzione.

Ore 11:30

XXXV Congresso nazionale AIP-ITCS
riservato ai soci

Con il patrocinio di:
REGIONE TOSCANA
CONFASSOCIAZIONI Digital
Clusit
Camera di Commercio Firenze dal 1770 la casa delle imprese
Università di Pisa
Partner dell'evento:
EDP YOUR INFORMATION TECHNOLOGY PARTNER
DARKBOX CYBERSECURITY
RICOH imagine. change.