AIEA

ASSOCIAZIONE ITALIANA INFORMATION SYSTEMS AUDITORS

nota anche come

ISACA®

Capitolo di Milano

PRESENTA

Photo by Bernard Hermant on Unsplash

SOC, DNS, PRIVACY

Milano, 24 marzo 2020 14.30-18.30

Auditorium UniCredit Services
Via Livio Cambi, 1

LE RELAZIONI

Maurizio Spinelli

Pro e contro di un SOC interno vs esterno e focus sul business

Oggi è sempre più importante, all'interno di una organizzazione aziendale, la presenza di un SOC (interno o esterno). E' una delle funzioni vitali con processi di sicurezza, tecnologie e persone specializzate atti alla rivelazione, risposta e il contenimento di incidenti di cyber security interni ed esterni.
Un buon SOC è quello che supporta gli obiettivi di business aziendale e migliora il profilo di rischio di sicurezza dell'organizzazione stessa.
E' molto importante capire la differenza fra un SOC interno ed esterno con i relativi benefici e valori che apporta all'organizzazione per un ambiente sicuro in cui il business possa realizzare gli obiettivi principali in linea con la direzione strategica e visione dell'azienda.
Riporteremo dei suggerimenti per strutturare e argomentare una discussione col top management per ricevere i fondi per l'implementazione di un SOC interno o esterno.

Andrea Pasquinucci

Aspetti di Privacy e Sicurezza del Domain Name System (DNS e DNSSEC)

Il Domain Name System (DNS) è un protocollo che, insieme al Routing BGP, forma l'infrastruttura portante di Internet. Pur essendo stato disegnato negli anni '80 con altissime caratteristiche di scalabilità, affidabilità, disponibilità e resilienza, i necessari aspetti di autenticità, integrità e confidenzialità/privacy sono stati introdotti solamente negli ultimi anni. In questo intervento, dopo una breve rassegna del protocollo DNS, viene presentato DNSSEC, le sue funzionalità di sicurezza e il livello attuale di adozione. Viene anche fatta una breve discussione sugli aspetti di confidenzialità/privacy e i protocolli DNS-over-HTTPS (DoH), DNS-over-TLS (DoT) e DNSCrypt.

Giancarlo Butti

L'impianto documentale per la conformità al GDPR

Nel GDPR il principio di accountability richiede che il Titolare sia in grado di dimostrare in ogni momento la propria conformità. Questo implica la necessità di predisporre un rilevante numero di documenti, molto spesso implicitamente richiamati dalla normativa, e la capacità di mantenerli aggiornati, spesso in tempo reale, e di garantirne la coerenza. Anche la modalità di compilazione o il livello di dettaglio è importante. Ad esempio un dettaglio troppo elevato nella individuazione delle finalità di trattamento all'interno del Registro delle attività di trattamento comporta la loro corretta declinazione all'interno delle informative per gli interessati, l'individuazione delle corrette basi giuridiche ed altro ancora.
Deve essere quindi individuato un corretto livello di equilibrio fra tutti gli elementi che consenta da un lato una corretta rappresentazione della realtà e dall'altro la loro reale manutenibilità nel tempo.

I RELATORI

Maurizio Spinelli

Laureato in Scienze dell'Informazione all'Università di Milano. Esperienza internazionale, high-complex nell'ambito di Cyber Security Strategy, Risk Management, Compliance and Security protection-detection measures.
E' trainer su tematiche come Cyber Security Risk and Compliance Management in ambito IT e OT. Security Awareness Training / Phishing Simulation, Incident and Response Management, and Data Privacy-Protection.
Utilizza security frameworks quali COBIT, NIST, SANS, CST, MITRE, ISO, COSO, PMI and ITIL ed è certificato CISA, CISM, CRISC, CSX and ITIL.

Andrea Pasquinucci (UCCI.IT)

Andrea Pasquinucci (PhD CISA CISSP) è un consulente freelance in sicurezza informatica. Si occupa prevalentemente di consulenza al top management in Cyber Security e di progetti, governance, risk management, compliance, audit e formazione in sicurezza IT.
E' socio AIEA ed ISACA, è socio fondatore ed è stato membro del Comitato Direttivo di AIPSI, è socio IEEE, è stato membro del Comitato Direttivo e del Comitato Tecnico Scientifico CLUSIT.

Giancarlo Butti

Ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Auditor, security manager ed esperto di privacy.
Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Ha erogato oltre 120 corsi e seminari presso presso ISACA/AIEA, ORACLE/CLUSIT, ITER, INFORMA BANCA, CONVENIA, CETIF, IKN, UNIVERSITA DEGLI STUDI DI MILANO
Già docente del percorso professionalizzante ABI - Privacy Expert e Data Protection Officer e master presso diversi atenei, ha all'attivo oltre 800 articoli e collaborazioni con oltre 30 testate.
Ha pubblicato 23 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 13 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT...
Socio e già proboviro di AIEA è socio del CLUSIT e del BCI.
Partecipa a numerosi gruppi di lavoro ed è fra i coordinatori di www.europrivacy.info.
Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, ISM, DPO, CBCI, AMBCI.

IL PROGRAMMA

14:00	Registrazione dei partecipanti
14:15	Saluti e introduzione
14:30	*Maurizio Spinelli* Pro e contro di un SOC interno vs esterno e focus sul business
15:30	*Andrea Pasquinucci* Aspetti di Privacy e Sicurezza del Domain Name System (DNS e DNSSEC)
16:30	Coffee Break
16:45	*Giancarlo Butti* L'impianto documentale per la conformità al GDPR
17:45	Dibattito con i Relatori
18:15	Conclusioni e networking

LUOGO E DATA

Martedì, 24 marzo 2020

Auditorium UniCredit Services s.c.p.a.
Via Livio Cambi, 1 – 20151 Milano (MM1 Lampugnano)

ISCRIZIONI

Soci AIEA

Portale delle Sessioni di Studio
https://portale.aiea.jed.st/

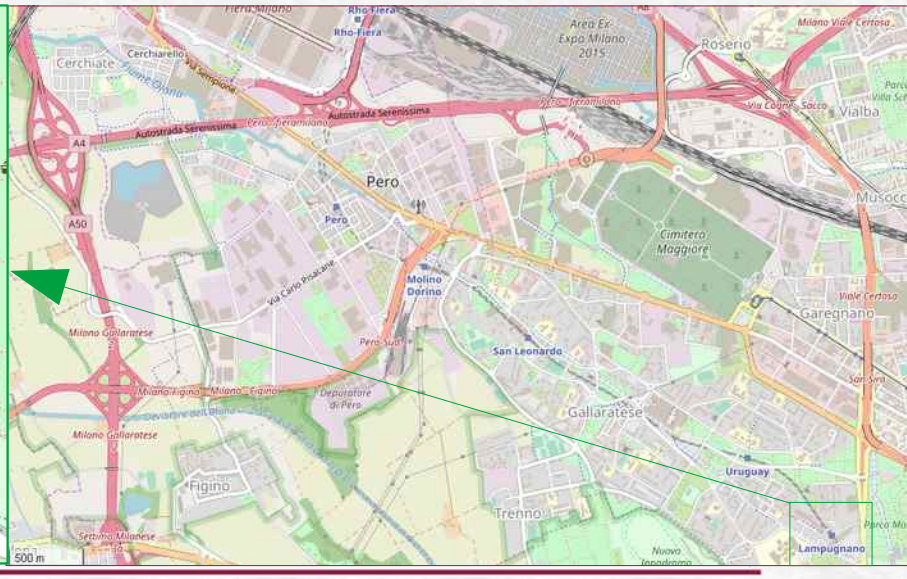
Se al primo accesso, recuperare la propria ISACA ID (numerica) dal sito ISACA o dalle comunicazioni di iscrizione/rinnovo e farsi inviare la password all'indirizzo preregistrato tramite la funzione
Password dimenticata

Non Soci

Contattare la segreteria AIEA per associarsi o versare il contributo organizzativo per il singolo evento
Segreteria AIEA

INDICAZIONI STRADALI

L'Auditorium di UniCredit Services si trova a poche decine di metri dalla fermata Lampugnano della MM1 (Linea rossa) di Milano e dall'omonimo Parcheggio di Corrispondenza ATM collegato da un raccordo all'uscita Milano Certosa dell'autostrada A4.



Associazione Italiana Information Systems Auditors

L'Associazione Italiana Information Systems Auditors è stata costituita a Milano nel 1979 con lo scopo di promuovere l'approfondimento dei problemi connessi con il controllo del processo di elaborazione automatica dei dati e di favorire lo sviluppo di metodologie e tecniche uniformi per la loro soluzione.

In particolare, gli obiettivi dell'Associazione sono:

- promuovere un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo, di affidabilità dell'organizzazione, Information Systems e di sicurezza dei sistemi;
- ampliare la conoscenza ed esperienza dei suoi oltre 800 membri nel campo dell'IT Governance, IT Security, Information Systems Auditing e Risk Control, favorendo lo scambio di metodologie per lo studio e la soluzione dei problemi inerenti;
- promuovere a livello nazionale la partecipazione alle certificazioni CISA, CISM, CGEIT, CRISC, CobiT e CSX

AIEA è associata da 40 anni ad ISACA, primo Capitolo in Europa, diventando nota internazionalmente come

ISACA®

Sistemi informativi: averne fiducia e trarne valore

Capitolo di Milano

ISACA® per i suoi oltre 135,000 soci in 188 paesi e per la comunità dei professionisti IT è fonte affidabile di possibilità di networking, certificazioni professionali, conoscenza e standard negli ambiti IT Governance, Cybersecurity, IT Risk e Assurance

www.aiea.it

20123 Milano - Via privata del Gonfalone, 3 - E-mail: aiea@aiea.it
Sito web: www.aiea.it – www.isaca.mi.it - P.IVA n. 10899720154 - C.F. n. 97109000154