AIEA

ASSOCIAZIONE ITALIANA INFORMATION SYSTEMS AUDITORS

nota anche come

ISACA Milan Chapter

PRESENTA

SICURI NEL RISCHIO

SICUREZZA ZERO TRUST, BUSINESS CONTINUITY, RISK QUANTIFICATION

Milano, 25 settembre 2020 14.30-18.30

online in streaming

in attesa di poter tornare nell'Auditorium UniCredit Services - Milano

IL PROGRAMMA

14:15	**Saluti e introduzione**
14:30	***Simona Di Felice, Daniel Rozenek*** **Modelli di sicurezza "Zero Trust": cosa sono e perché le aziende dovrebbero adottarli per proteggersi in un contesto mutato**
15:30	***Roberto Dellavedova*** **Tecnologie e strumenti per costruire una strategia completa di Business Continuity**
16:30	**Coffee Break**
16:45	***Giancarlo Butti, Alberto Piamonte*** **Metodologie per il Risk Quantification. Un approccio al metodo FAIR**
17:45	**Dibattito con i Relatori**
18:15	**Conclusioni e networking**

LE RELAZIONI

Simona Di Felice, Daniel Rozenek

Modelli di sicurezza “Zero Trust”: cosa sono e perché le aziende dovrebbero adottarli per proteggersi in un contesto mutato

La trasformazione digitale, l’utilizzo sempre più spinto di soluzioni SaaS e del Cloud, l’esperienza pandemica Covid-19 e l’adozione dello smartworking in modalità prevalente hanno messo in luce le debolezze dei modelli di sicurezza tradizionali. Questi fenomeni, che rappresentano ormai una realtà ineludibile per molte aziende, hanno infatti un’incidenza significativa sulla superficie di attacco - sempre più estesa - e sulle attuali architetture di rete e sicurezza, non più in grado di controllare un ecosistema così complesso, favorendo attacchi e attività cybercriminali.
In questo contesto mutato, occorre che le decisioni relative alla sicurezza e all'accesso siano applicate dinamicamente in base a identità, dispositivi e al contesto dell'utente e che solo gli utenti e i dispositivi autenticati e autorizzati possano accedere ad applicazioni e dati.
Questo, per le aziende, potrebbe essere il momento giusto per considerare l’adozione di un approccio Zero Trust.

Roberto Dellavedova

Tecnologie e strumenti per costruire una strategia completa di Business Continuity

Sicurezza ed alta disponibilità dei dati sono temi sempre attuali all'interno delle aziende. Backup e replica sono importanti per Business Continuity e Disaster Recovery ma non sono sufficienti. In questa sessione discuteremo le metodologie più efficaci per implementare una strategia che garantisca una completa disponibilità e protezione dei dati. Vedremo come ottimizzare i processi di Business Continuity e Disaster Recovery sfruttando tecnologie in grado di verificare la consistenza dei dati e semplificare i processi di ripristino.

Giancarlo Butti, Alberto Piamonte

Metodologie per il Risk Quantification. Un approccio al metodo FAIR

L’analisi dei rischi è un’attività fondamentale quale strumento per identificare le aree dove è prioritario intervenire con delle opportune contromisure.
Diventa quindi fondamentale da un lato la capacità di recuperare le informazioni necessarie per effettuare una stima attendibile dei possibili impatti sulle varie tipologie di asset che interessano l’azienda, le conseguenze dirette ed indirette sull’organizzazione, le conseguenze sui diritti e libertà delle persone fisiche…
Analogamente si deve procedere per la corretta individuazione degli scenari di rischio, la loro probabilità di accadimento e la probabilità che il verificarsi di tali eventi abbia effettivo impatto sugli asset e sull’azienda.
Una corretta valutazione non può tuttavia basarsi su semplice valutazione di natura qualitativa, ma è necessario un approccio che consenta una più precisa valutazione e rappresentazione dei singoli rischi e della loro aggregazione.
Ecco quindi il ricorso a metodologie che permettono una valutazione di natura quantitativa, quali FAIR (fra gli altri richiamate da ISACA nella ultima versione della Risk IT Practitioner Guide).

I RELATORI

Simona Di Felice (Sia Partners)

Da oltre 15 anni si occupa di IT, supportando il Management di grandi Organizzazioni appartenenti a diversi segmenti di mercato (Banche, Compagnie assicurative, Telco, aziende del settore manifatturiero e industriale, etc), nella definizione e realizzazione di complessi piani di trasformazione strategica, nel disegno, nell'implementazione e/o nella verifica di modelli di gestione dei rischi IT /Cyber, sistemi a supporto del governo e della sicurezza delle informazioni e della privacy e di ICT Compliance. Poiché ha piena consapevolezza della portata strategica del fattore "innovazione" per l'IT, conduce un'attività costante di ricerca sul mercato di soluzioni ad elevato tasso di innovazione, accompagnando le aziende nel processo di selezione e change management. Da anni, affianca all'attività di consulenza l'impegno didattico e formativo, che esercita presso primarie università e centri di ricerca, soprattutto nell'ambito della Data Governance/ Data Management, Cybersecurity e Data Protection. Ha lavorato presso importanti realtà internazionali del Management Consulting e, attualmente, è in Sia Partners, dove ricopre il ruolo di responsabile della practice "CIO Advisory".
È socio di Isaca e AIEA, certificata CISA e ISO 27001.

Daniel Rozenek (Tekapp)

Nato in Israele, laureato in Economia delle reti e della comunicazione ma con forte passione per il mondo IT. Da 15 anni si occupa di innovazione tecnologica, passando da responsabile area presso società informatiche per arrivare a fondarne una propria nel 2014. Tekapp vanta un team preparato e solido e sempre alla ricerca di nuove sfide. Unica azienda italiana a utilizzare il protocollo israeliano di cybersecurity. Tale protocollo permette di utilizzare approcci, procedure e strumenti software testati ed accuratamente selezionati nel mondo militare israeliano per garantire alle PMI italiane la migliore sicurezza informatica delle proprie infrastrutture. Scouting internazionale ha portato la sua azienda ad esserne una delle più vive e innovative del territorio in grado di sopperire alle esigenze e di rispondere alle necessità di qualsiasi impresa, dalla pmi alla multinazionale. Esperto di CyberSecurity, cura gli aspetti di consulenza e tecnologici del proprio parco clienti, diffondendo anche informazioni di carattere culturale su vari canali quali social, blog, giornali. Formatore su diversi corsi di cybersecurity rivolti ai dipendenti delle aziende. Attivo nel territorio Modenese è stato presidente dei giovani imprenditori di Confimi Emilia (Confimi Industria), socio attuale del CDO, dove viene riconosciuto e chiamato per tematiche di cybersecurity.

Roberto Dellavedova (Veeam)

A partire dal 2000 Roberto ha lavorato per alcuni dei maggiori vendor di tecnologie Storage, Backup e Disaster Recovery occupando vari ruoli. Attualmente copre il ruolo di Enterprise System Engineer in Veeam Italia.

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. 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 25 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 15 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.blog.europrivacy.info . Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI, AMCBI.

Alberto Piamonte (KeyMap)

Alberto Piamonte, laureato nell'Università di Padova in Ingegneria Elettronica, fa attualmente parte del KeyMap Team, un gruppo di Consulenti ed Aziende che si occupa dello sviluppo di strumenti automatizzati e metodologie per attività di audit, l'analisi e gestione dei rischi, la certificazione conformità e la realizzazione di efficaci ed efficienti sistemi di controllo e di governo. Oltre che svolgere in prima persona attività di consulenza si occupa attivamente dei problemi relativi al governo dei sistemi IT tenendo frequenti corsi e seminari su metodologie quali COBIT, ITIL, ISO27001 e GDPR ed alla sensibilizzazione e diffusione delle relative tematiche. Una lunga carriera nel mondo ICT con significative esperienze internazionali. Istruttore,Implementor e Assessor COBIT5,è attualmente Consigliere ISACA Capitolo di Roma.

LUOGO E DATA

Venerdì, 25 settembre 2020

Online sulla piattaforma di Streaming di AIEA

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

Un Socio AIEA invita un Non Socio

Ogni Socio AIEA può invitare un Non Socio, che potrà seguire lo streaming sulla pagina dedicata del Sito AIEA. Contattare Luca Pertile <luca.pertile@aiea.it> per la chiave di accesso.

Non Soci

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

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®
Milan Chapter

ISACA® per i suoi oltre 145,000 soci in oltre 180 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