ASSOCIAZIONE ITALIANA INFORMATION SYSTEMS AUDITORS

nota anche come

ISACA Milan Chapter

ORDINEdegliINGEGNERI
della
PROVINCIAdiSIENA

RSA SECURITY

PRESENTANO

con il patrocinio di

CONFASSOCIAZIONI Digital

AIP Associazione Informatici Professionisti

ITCS Italian Computer Society

La Teoria è nulla senza la Pratica..!!

Minacce, GDPR, CyberRisk

26 novembre 2021 14.00-18.00

Sessione di Studio in Streaming

PRESENTAZIONI

David Cecchi

Vulnerabilità e minacce: quale legame?

Durante questo incontro ci occuperemo di definire una "Minaccia" e ne analizzeremo un po' più in dettaglio qualcuna.
Daremo una definizione di Vulnerabilità e faremo degli esempi cercando di capire come queste ultime influenzino gli attaccanti.
Verificheremo "dal vivo" come sia possibile eseguire una scansione di un Target utilizzando GSA e ne commenteremo i risultati.

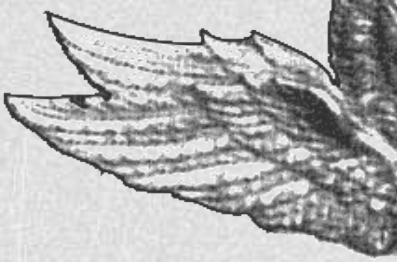
Giancarlo Butti

La doppia visione dei rischi nel GDPR

L'analisi del rischio nel GDPR (termine che non compare mai nel testo di legge) presenta delle peculiarità che la contraddistinguono:

- *non riguarda un rischio aziendale (motivo per cui i tradizionali metodi di analisi utilizzati ad esempio per la 27001 non sono conformi); quello che deve essere valutato è il rischio per i diritti e libertà delle persone fisiche*
- *non riguarda la sola sicurezza (art. 32), ma anche altri aspetti (artt. 24 e 25)*
- *è sempre obbligatoria*
- *non va confusa con la DPIA*
- *è difficile una precisa quantificazione considerando che, ad esempio, non è noto il numero di persone fisiche che possono subire un danno (al più possono essere noti gli interessati).*

Accanto a queste analisi obbligatorie, nulla vieta che il Titolare possa contestualmente effettuare una valutazione del proprio rischio, in termini in particolare di rischio sanzionatorio e rischio risarcitorio (che si sommano agli altri numerosi rischi derivanti ad esempio dalla indisponibilità dei dati).
L'intervento si propone quindi di trattare entrambe queste visioni, per consentire una più adeguata valutazione complessiva del rischio, indispensabile per una corretta valutazione di adeguate contromisure.



Luciano Veronese, RSA Security

Cyber Risk Quantification: communicate Cyber Risk in business terms

Cyber Risk relevance is constantly on the rise and in recent years this topic has become a board-level discussion. As a result, Cyber Risk is now recognized as a fundamental component of Business Risk. Traditionally Cyber Risk has been evaluated using a simple qualitative risk scoring approach using “high/medium/low" values, but business stakeholders speak in the language of “numbers and money”. Business stakeholders want to know loss exposure due to a potential cyber event or the ROI of purchasing security controls and CISOs are struggling to articulate Cyber Risk in this language and provide meaningful answers to the executives and board members.

This presentation looks at a quantitative risk assessment approach using financial terms easily understood by business leaders and by talking the same language are able to bridge the gap between the domains of security and business functions. By filling this historical communication gap organizations increase the effectiveness of the decision-making process related to security spending.

Cyber Risk quantification is becoming mainstream and many regulatory bodies are looking at mandating its adoption or have already done so. Moreover, as Digital Transformation ramps up, auditors will increasingly encounter organizations adopting this approach. This session will arm you with the knowledge to exploit a business-driven approach and have the right conversation.

AGENDA

14:00 – 14:10

Avvio streaming

14:10 – 14:20

Saluti del Presidente di AIEA

14:20 – 15:10

David Cecchi

Vulnerabilità e minacce: quale legame?

15:10 – 16:00

Giancarlo Butti

La doppia visione dei rischi nel GDPR

16:00 – 16:30

Coffee break

16:30 – 17:20

Luciano Veronese, RSA Security

Cyber Risk Quantification: communicate Cyber Risk in business terms

17:20 – 18:00

Confronto e dibattito

18:00

Conclusione e ringraziamenti

RELATORI

David Cecchi

CyberSecurity Specialist, si occupa attualmente di tematiche relative alla CyberSecurity Governance. In precedenza ha lavorato per 4 anni nella componente tecnica/tecnologica della Sicurezza IT MPS e prima ancora si è occupato, per circa 15 anni, di progettazione e realizzazione di Architetture di livello Enterprise.

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 130 corsi e seminari presso ISACA/AIEA, Oracle/Clusit, Iter, Informa Banca, Convenia, Cetif, Ikn, Università degli studi Di Milano, Università di Napoli, Cefriel. 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 19 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 BS7799, ISO/IEC27001, CRISC, CDPSE, ISM, DPO, CBCI e AMBCI.

Luciano Veronese, RSA Security

Tech professional for about 30 years and in this he amassed a huge range of IT and security industry experience, most of them operating in the technical pre-sales function for multinational companies. In the last 9 years focused exclusively on GRC technologies (RSA Archer) covering all the typical Governance Risk and Compliance domains (Risk Management, Regulatory Compliance, Business Resiliency, Internal Audit, IT and Security Risk, Third Part Risk and more). He has the technical responsibility of positioning the RSA GRC portfolio across Europe (and particularly in Italy, Spain, Israel and Greece) supporting both the RSA sales force and partners in RFPs, presentations, and Proof of Concept developments. Specialized in IT/InfoSec and Operational Risk Management and recently passed the FAIR certification (from the Open Group) which is the leading Cyber Risk Quantification methodology.
Regularly speaks at both public and company conferences and events across EMEA.

ISCRIZIONE

Soci AIEA

*L'iscrizione all'evento, gratuita, deve essere completata sul Portale delle Sessioni di Studio AIEA, all'indirizzo **https://portale.aiea.jed.st/** entro e non oltre il 25 novembre 2021. La partecipazione all'evento dà diritto ad acquisire 4 CPE per mantenere le certificazioni CISA, CISM, CGEIT e CRISC.*

Ordine degli Ingegneri

*L'iscrizione all'evento deve essere completata sul portale della Formazione Continua dell'Ordine degli Ingegneri della Provincia di Siena **http://siena.ing4.it/**. La partecipazione all'evento dà diritto ad acquisire **3 CFP**.*

*La partecipazione all'evento richiede un contributo di **5 Euro**.*

Non Soci

*La partecipazione all'evento richiede un contributo di **10 Euro**. Per iscriversi contattare la Segreteria AIEA all'indirizzo email aiea@aiea.it entro e non oltre il 25 novembre 2021.*

*L'evento è **gratuito per gli studenti** e **per i soci delle associazioni patrocinanti.***

ISACA®
Milan Chapter

ORDINE degli INGEGNERI della PROVINCIA di SIENA

L'Ordine è un Ente pubblico Non Economico, ausiliario dello Stato, istituito con Legge Ordinaria.

All'Ordine sono attribuite specifiche competenze; è sottoposto al controllo ed alla vigilanza da parte del Ministero di Grazia e Giustizia, presso il quale è stabilita la sede del Consiglio Nazionale CNI

L'Ordine tiene aggiornato l'elenco degli iscritti nell'Albo Professionale.

La professione di Ingegnere, nei sui vari indirizzi, rientra tra le cosiddette professioni protette; ciò significa che per essere legittimati ad esercitare è necessaria l'iscrizione al relativo albo.
L'Ordine professionale da un lato si fa garante dell'accesso all'esercizio della professione di Ingegnere solo da parte di soggetti in possesso dei requisiti richiesti dalla legge, dall'altro lato esercita controllo sui propri iscritti, richiedendo loro che mantengano un comportamento rispondente alla deontologia professionale.

L'Ordine è totalmente sostenuto dai contributi degli iscritti, conferiti provincia per provincia

http://ording.si.it/

Ordine degli Ingegneri della Provincia di Siena
info@ording.si.it

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 alla 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 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