AIEA ASSOCIAZIONE ITALIANA INFORMATION SYSTEMS AUDITORS

nota anche come

ISACA Milan Chapter

PRESENTA

Esame	Risultato	Unit.Mis.	Valori di Riferimento
EMOCROMO			
Contaglobuli automatica			
WBC (Leucociti)	**5,8**	x10^3/mmc	4.3-10.0
NEU% (Granulociti neutrofili)	**62,1**	%	40-75
LYM% (Linfociti)	**26,8**	%	19.0-48.0
MON% (Monociti)	**7,8**	%	1.0-10.0
EOS% (Granulociti eosinofili)	**3,3**	%	0.0-6.0
BAS% (Granulociti basofili)	**0,0**	%	0.0-1.5
NEU#	**3,61**	x10^3/mmc	1.8-7.0
LYM#	**1,56**	x10^3/mmc	1.0-4.8
MON#	**0,45**	x10^3/mmc	0.1-0.8
EOS#	**0,19**	x10^3/mmc	0.0-0.45
BAS#	**0,00**	x10^3/mmc	0.0-0.2

4 Ore CPE

Quale protezione per le informazioni sulla nostra salute?

Torino, 17 giugno 2022 9.00-13.00

Online in Streaming

in attesa di poter tornare in Corso Lione 24 - 10141 Torino

IL PROGRAMMA

09:00	Saluti e introduzione *Stefano Niccolini, Presidente AIEA*
09:15	*Danilo Diomede (RINA)* Eventi ed incidenti di sicurezza delle informazioni nell'healthcare
10:00	*Giuliano Fabbrini e Federica Foti (RINA)* Cybersecurity protection healthcare
11:00	Break
11:30	*Omar Khan (RINA)* L'approccio di sistema alla sicurezza delle informazioni e alla cyber security nell'ambito Healthcare
12:30	Dibattito con i Relatori
13:00	Termine lavori

LE RELAZIONI

Danilo Diomede (RINA)

Eventi ed incidenti di sicurezza delle informazioni nell'healthcare

La crescente digitalizzazione delle informazioni scambiate nell'Healthcare, sia all'interno delle strutture sanitarie che in spazi virtuali aperti anche agli utenti, rappresenta un passo avanti nel progresso della ricerca medica e dell'erogazione dei servizi.
D'altro canto, la cronaca riporta con frequenza crescente il verificarsi di incidenti di sicurezza delle informazioni dovuti ad attacchi rivolti a strutture sanitarie, con conseguenze immediate sull'interruzione dei servizi erogati ai pazienti/utenti, ma anche con impatti meno immediati, ma persino più gravi, sulla protezione dei dati personali sanitari, che spesso vengono "catturati" dagli attaccanti per chiedere un "riscatto" ai fini del loro rilascio, oppure sono messi in vendita sul dark web per scopo di lucro.
Riconoscendo che l'approccio alla gestione delle informazioni nel settore sanitario è in buona parte ancora legato a logiche non basate sul valore delle informazioni e sui rischi cui sono soggette, l'intervento mira ad inquadrare la problematica all'interno del framework ISO/IEC 27001, diffusa norma certificabile focalizzata sull'information security, a partire dalle definizioni stesse di "sicurezza delle informazioni", di "evento" e di "incidente". L'analisi delle specifiche tipologie di dati ed informazioni scambiate nel perimetro degli operatori di Healthcare, incrociate col racconto dei recenti incidenti verificatisi in Italia e nel mondo, permetterà di delineare il "profilo di rischio" di tali informazioni, in modo da favorire negli operatori una crescita di consapevolezza del rischio e delle responsabilità connesse allo scambio di informazioni, per sviluppare un nuovo approccio proattivo e sistemico alla protezione delle informazioni e dei dati.

Giuliano Fabbrini e Federica Foti (RINA)

Cybersecurity protection healthcare

Le infrastrutture critiche, che includono le strutture ospedaliere, sono elementi molto sensibili a tutto quello che concerne le tematiche di cyber security. Il numero di attacchi è in forte aumento sia nelle strutture private che pubbliche.
La normativa NIS prevede linee guida e obblighi normativi che ogni infrastruttura critica deve rispettare.
Sia per motivi normativi che per esigenze di resilienza molti ospedali stanno lavorando per migliore la propria postura Cyber Security. A tal proposito presenteremo la nostra esperienza nel disegnare e implementare soluzioni di cyber security in ambito sanitario, grazie al coinvolgimento continuo di tre centri sanitari europei (uno in Italia, uno a Creta e uno in Irlanda) e vari stakeholders del settore nella valutazione della sicurezza informatica, e la preparazione sia delle infrastrutture IT sanitarie che dei dispositivi medici connessi.
Tali soluzioni prevedono strumenti tecnologici (legati a valutazione dinamica e la mitigazione del rischio, condivisione sicura delle informazioni, security-by-design di dispositivi medici, identificazione e autenticazione di staff e dispositivi) e strumenti organizzativi (legati a formazione e l'educazione del personale sanitario, politica organizzativa e modelli decisionali per l'adozione di comportamenti sicuri).
A supporto di una efficace adozione degli strumenti citati all'interno del perimetro ospedaliero, sono state inoltre sviluppate linee guida di implementazione e metodologie per valutare il ritorno di investimento (RoI) degli interventi di cybersecurity.

Omar Khan (RINA)

Approccio di sistema alla sicurezza delle informazioni e alla cyber security nell'healthcare

Le problematiche che si trovano ad affrontare, con sempre maggiore frequenza, le organizzazioni che gestiscono informazioni, suggeriscono di abbandonare un approccio reattivo e tecnico-specialistico, basato cioè sull'adozione di contromisure specifiche nei confronti delle minacce per la sicurezza delle informazioni trattate in ambito ospedaliero e sanitario, in favore di un approccio proattivo e sistemico, tipico dei sistemi di gestione ampiamente utilizzati in ambito industriale e dei servizi.
L'adozione di un sistema di gestione volto a tutelare la riservatezza, l'integrità e la disponibilità delle informazioni gestite dalle strutture sanitarie è uno sforzo necessario, considerando il valore di tali informazioni, sia in relazione agli obblighi di legge nella tutela della privacy, che per via della valore intrinseco delle informazioni sanitarie che talvolta trovano un mercato illecito sul darkweb.
Il focus delle organizzazioni sanitarie deve quindi spostarsi dalla gestione tecnica dell'ambito IT, molte volte considerata un'estensione dei servizi infrastrutturali di ingegneria clinica (e.g. condizionamento e gas sanitari) all'impostazione di piani di trattamento del rischio di perdita delle già menzionate proprietà fondamentali delle informazioni.
Le norme sviluppate al riguardo dall'ISO - imperniate sullo standard certificabile ISO/IEC 27001 – sono utilmente integrate da linee guida specifiche per l'implementazione dei controlli di sicurezza (ISO/IEC 27002), per l'estensione dell'information security alla gestione dei dati personali (ISO/IEC 27799) e per la definizione di un perimetro di cybersecurity in cui le informazioni e gli asset (im)materiali che le veicolano possano garantire livelli di sicurezza in grado di fronteggiare i rischi individuati in fase di risk assessment.

I RELATORI

Danilo Diomede

Ingegnere elettronico, appassionato di tecnologia ed organizzazione, di cui si è occupato in alcune esperienze consulenziali e di ricerca. Da vent'anni opera nel campo dell'auditing e della formazione su schemi normativi relativi alla qualità e all'information security (ISO 9001, ISO 22301, ISO/IEC 27001), anche in veste di Account Manager. Lead Auditor certificato da AICQ-SICEV.

Giuliano Fabbrini

Giuliano Fabbrini è entrato a far parte di RINA Consulting nel 2018, con il ruolo di Sales Manager per la Unit Industry.
Da gennaio 2022 ricopre il ruolo di Business Development Manager Cyber and Physical Security per la Unit Cyber di Rina Consulting.
Le maggiori attività sono:

- Gestione del rapporto commerciale con i clienti
- Responsabile per attività di sviluppo business.
- Selezione di partner strategici

Federica Foti

Federica Foti got her Master Degree in Bioengineering in 2018 from the University of Genoa. She joined RINA Consulting (formerly D'Appolonia) in 2019, where she became part of the Italy Integrated Security Unit working as analyst and software developer. At the moment she is part of a new division in RINA with the role of Governance Risk & Compliance analyst. Since the beginning, she has been involved in specific EU projects, in particular "PANACEA: Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people", both as contributor and WP leader, working under different perspectives such as deliverables preparation, SW development and coordination of the work of the partners involved. The main activities were focused on cybersecurity aspects, such as:

- Analysis of cybersecurity and HealthCare standards and regulations;
- Accurate study of the risk scenarios involved in the Healthcare domain in order to underline cybersecurity aspects within it;
- Conformity assessment to identify the compliance with the defined security requirements for different organizations/companies.

Her profile combines cyber security, biomedical and software aspects acquired through both work and university experience.

Omar Khan

Omar holds an MBA from London Business School - United Kingdom and an M. Sc. in Electronic Engineering from University of Genoa – Italy.
He read behavioral economics at Columbia Business School, New York (US), merge and acquisitions and game theory at UCLA Anderson School of Management, Los Angeles (US).
Well versed in IT project and service management, he joined RINA in 2019 as a digital process improvement manager after a long and eclectic career in several multinationals and SMEs around Europe, Asia and South America.
He is an ISO27001 auditor, a CISA and an AIEA/ISACA member.
He is also active in some not-for-profits initiatives among which the London-based organization "The Wings of Hope Children's Charity" mentoring schoolchildren in improving their transferable skills such as project management and leadership.

LUOGO E DATA

Venerdì, 17 giugno 2022

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 invita un Non Socio

Ogni Socio AIEA può invitare un Non Socio, che potrà seguire lo streaming sulla pagina dedicata del Sito AIEA. Contattare Daniela Cellino <daniela.cellino@aiea.it> per la chiave di accesso.

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 oltre 40 anni ad ISACA, primo Capitolo in Europa, diventando nota internazionalmente come

ISACA® Milan Chapter

ISACA® per i suoi oltre 165,000 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