

Nome e cognome

CLAUDIO TELMON

Profilo

IT SECURITY CONSULTANT

Esperienza

25 ANNI

RIEPILOGO

Claudio Telmon, Information & Cyber Security Advisor, è da oltre 20 anni consulente freelance nel campo della sicurezza informatica. Ha gestito il laboratorio di sicurezza del Dipartimento di Informatica dell'Università di Pisa, ed in seguito ha continuato a collaborare con il Dipartimento per attività di didattica e di ricerca, oltre ad aver fatto parte dei gruppi di lavoro di ENISA, European Network and Information Security Agency. Si è occupato come professionista dei diversi aspetti tecnologici e organizzativi della sicurezza, lavorando per aziende del settore finanziario, delle telecomunicazioni e per pubbliche amministrazioni con forte expertise nell'ambito sanitario e ospedaliero.

Attualmente svolge attività di consulenza sui diversi aspetti della sicurezza ICT, che comprendono il supporto alla gestione del rischio, la predisposizione di strutture per la gestione degli incidenti, l'audit e risk assessment su sistemi informativi di aziende private e pubbliche amministrazioni oltre che nel supporto nella definizione di Sistemi di Gestione della Sicurezza Informatica, comprese l'analisi dei requisiti e la definizione di ruoli, politiche e procedure. L'attività recente riguarda principalmente il settore della sanità, che segue specificamente da circa dieci anni.

È membro del Comitato Direttivo del CLUSIT, con delega per l'Agenda Digitale. Nell'ambito delle attività dell'associazione è anche responsabile: dei Progetti Europei, dei Progetti per le PMI, del Premio Tesi, ed ha gestito per conto del CLUSIT la partecipazione al progetto europeo EISPP, curando gli aspetti tecnici e organizzativi nonché i rapporti con i partner e la Commissione Europea. Per Clusit ha partecipato nel 2019 al gruppo di esperti per la definizione della strategia nazionale per l'intelligenza artificiale del Ministero per lo Sviluppo Economico.

ESPERIENZA LAVORATIVA

- Date (da – a)
- Nome e indirizzo datore di lavoro
- Tipo di impiego
- Principali mansioni e responsabilità

1997 – ALLA DATA ATTUALE

Libero professionista

Consulente e adviser nel campo della sicurezza e dell'audit ICT

La mia attività lavorativa ha coperto nel tempo i diversi aspetti della sicurezza ICT, comprendendo quelli di gestione e configurazione dei sistemi, lo sviluppo di software, l'audit, la progettazione e implementazione di ISMS, la formazione, la ricerca, fino alle problematiche ICT relative alla Business Continuity. Questi aspetti sono stati esposti come attività di consulenza, come affiancamento al personale aziendale, come gestione di gruppi di lavoro e di ricerca e come gestione complessiva della partecipazione a progetti europei.

Attività recenti comprendono:

- l'analisi dei rischi in logica security by design e data protection by design per la realizzazione di nuovi servizi e trattamenti, in particolare in ambito sanitario
- il supporto all'analisi dei requisiti di sicurezza per dispositivi medici, anche in conformità con il regolamento MDR
- l'audit di fornitori, in relazione ai requisiti di sicurezza e di protezione dei dati personali
- il supporto alla conformità alla normativa sul trattamento dati personali (GDPR);
- l'analisi dei rischi IT e di sicurezza IT in ambito Industry 4.0;
- il supporto alla conformità di gruppi bancari e dei loro fornitori alla normativa di Banca d'Italia, anche in termini di adeguamento del modello organizzativo per la gestione della sicurezza IT;
- la definizione di schemi di politiche e procedure per la gestione della sicurezza delle informazioni, anche nell'ambito di Sistemi di Gestione della sicurezza delle Informazioni (SGSI);
- il supporto a medie imprese di diversi settori (manifatturiero, software house...) nell'individuazione delle esigenze di gestione della sicurezza IT e cybersecurity;
- il supporto alla conformità alla normativa PCI;
- la definizione e analisi di protocolli per le transazioni online;
- il supporto nella predisposizione di strutture per la gestione degli incidenti;

- la partecipazione a gruppi di lavoro relativi alla sicurezza IT in ambito socio-sanitario;
- attività di formazione e sensibilizzazione a tutti i livelli;
- attività di social engineering (es. spear phishing) a supporto dell'attività di formazione.

- Date (da – a)
- Nome e indirizzo datore di lavoro
- Tipo di impiego
- Principali mansioni e responsabilità

2009 – 2011

Università di Pisa e La Spezia

Docente a contratto

- Anno Accademico 2009/2010: Docente a contratto di “Metodi e Strumenti per la sicurezza” per la Laurea Magistrale in Sicurezza Informatica, Università di Pisa, polo di La Spezia
- Anno Accademico 2010/2011: Docente a contratto di “Crittografia avanzata” per la Laurea Magistrale in Sicurezza Informatica, Università di Pisa, polo di La Spezia

- Date (da – a)
- Nome e indirizzo datore di lavoro
- Tipo di impiego
- Principali mansioni e responsabilità

2002 – ALLA DATA ATTUALE

CLUSIT

Membro del Comitato Direttivo

- Membro del Comitato Direttivo di CLUSIT - Associazione Italiana per la Sicurezza Informatica
- Membro del Comitato Tecnico Scientifico di CLUSIT

- Date (da – a)
- Nome e indirizzo datore di lavoro
- Tipo di impiego
- Principali mansioni e responsabilità

2005 – 2009

AIPSI

Membro del Comitato Direttivo di AIPSI

- Socio Fondatore e Membro del Comitato Direttivo di AIPSI - Associazione Italiana Professionisti della Sicurezza Informatica

- Date (da – a)
- Nome e indirizzo datore di lavoro
- Tipo di impiego
- Principali mansioni e responsabilità

1997 – 2005

Università di Pisa

Responsabile tecnico del Laboratorio di Sicurezza del Dipartimento di Informatica dell'Università di Pisa

- L'attività prevedeva la gestione sistemistica del laboratorio ed il supporto allo svolgimento dei progetti da parte di gruppi di studenti

ISTRUZIONE E FORMAZIONE

- Data (da – a)
- Titolo di Studio
- Nome e tipo di istituto di istruzione

Luglio 1995

Laurea in Scienze dell'Informazione

Università degli Studi di Pisa, Pisa (PI)

In possesso delle certificazioni: CISSP - Certified Information Systems Security Professional

Iscritto all'elenco degli Esperti di Innovazione Tecnologica del MISE

CAPACITÀ E COMPETENZE PERSONALI

MADRELINGUA **ITALIANA**

ALTRA LINGUA **INGLESE**

• Livello **C1**

ALTRE LINGUE **TEDESCO, FRANCESE, SPAGNOLO: CONOSCENZA DI BASE**

CAPACITÀ E COMPETENZE
ORGANIZZATIVE**Project Management**

Nel corso dell'attività di consulenza ho partecipato a progetti e gruppi di lavoro nei diversi ruoli, compresa la gestione di gruppi di lavoro (fino a 10 persone) in progetti di durata breve o media per attività di sviluppo software e security assessment.

Dal 1997 al 2005, nel ruolo di responsabile tecnico del Laboratorio di Sicurezza del Dipartimento di Informatica dell'Università di Pisa, oltre alla gestione sistemistica del laboratorio, l'attività ha comportato il supporto allo svolgimento dei progetti, sia di tipo sistemistico che di sviluppo software, da parte di gruppi di studenti.

Dal 2002 al 2004 ho gestito per conto del CLUSIT la partecipazione al progetto europeo EISPP, curando gli aspetti tecnici e organizzativi nonché i rapporti con i partner e la Commissione Europea.

CAPACITÀ E COMPETENZE
TECNICHE

La mia attività lavorativa ha coperto nel tempo i diversi aspetti della sicurezza ICT, comprendendo quelli di gestione e configurazione dei sistemi, lo sviluppo di software, l'audit, la progettazione e implementazione di ISMS, la formazione, la ricerca, fino alle problematiche ICT relative alla Business Continuity.

Ho inoltre approfondito il tema della sicurezza IT in particolare in ambito sanitario e ospedaliero, anche partecipando per Clusit a gruppi di lavoro AISIS (Associazione Italiana Sistemi Informatici in Sanità), nei quali ho contribuito alla sezione relativa alla sicurezza IT.

Problematiche tecniche affrontate comprendono:

- assessment e supporto all'adeguamento ai requisiti di sicurezza posti da diverse norme e linee guida: GDPR, ISO/IEC 27001 e standard collegati, CSA-CCM, NIST SP 800-53, NIST SP 800-82, linee guida AgID; l'attività è stata svolta su sistemi IT e OT di diversi settori: manifatturiero, utility, sanità, bancario, servizi
- supporto alla conformità di gruppi bancari alla normativa bancaria vigente
- supporto alla gestione del rischio nell'utilizzo di servizi in cloud
- definizione di protocolli per le transazioni online
- supporto nella predisposizione di strutture per la gestione degli incidenti
- attività dimostrative di spear phishing a supporto dell'attività di sensibilizzazione per grandi aziende
- audit e risk assessment su sistemi informativi di aziende private e pubbliche amministrazioni
- supporto nella definizione di un Sistema di Gestione della Sicurezza Informatica, comprese l'analisi dei requisiti e la definizione di ruoli, politiche e procedure
- gestione e prevenzione di attacchi di Denial of Service distribuito
- soluzioni di autenticazione biometrica
- soluzioni per la sicurezza in ambiente SCADA e in sistemi di monitoraggio in ambiente industriale
- problematiche di firma digitale e di interoperabilità fra pubbliche amministrazioni
- problematiche di business continuity
- analisi delle problematiche di tutela dei dati personali;
- supporto nella predisposizione di bandi di gara nell'ambito della sicurezza ICT

Fra il 2008 e il 2009 ho inoltre partecipato a gruppi di lavoro di ENISA, European Network and Information Security Agency. Partecipo a progetti europei di innovazione finanziati dalla Commissione Europea.

Fra il 2005 e il 2008, con la società Next-Hop, attività di studio, progettazione e formazione nel campo delle tecnologie avanzate di networking, con particolare attenzione alle problematiche di sicurezza e business continuity.

Consulenza

Consulenza nel campo della sicurezza dei sistemi informatici relative ad aziende di rilevanza nazionale e internazionale, istituti di ricerca, enti pubblici e ISP. anche in collaborazione con società specializzate nel settore. L'attività attuale riguarda principalmente:

- l'analisi e audit della gestione della sicurezza ICT, e l'indicazione di azioni correttive, sia tecniche che organizzative, in riferimento agli standard e good practice del settore;
- l'analisi del rischio;
- la progettazione e configurazione di meccanismi di sicurezza;
- il supporto alla gestione e analisi di incidenti di sicurezza;
- la formazione del personale

Progettazione software

Ho svolto in passato attività di progettazione di software per la sicurezza delle reti, sia sperimentale che commerciale. L'attività svolta riguarda in particolare:

- componenti per sistemi firewall;
- componenti di Public Key Infrastructure;
- componenti per sistemi di Intrusion Detection.

Attività sistemistica

Fino al 2005 ho svolto anche attività sistemistica su reti di dimensioni medio/piccole. Nel seguito ho mantenuto le competenze necessarie per le attività di base di gestione dei sistemi. Le competenze in quest'area comprendono:

- gestione di reti locali in ambiente misto Windows/Unix/Linux
- conoscenza approfondita dei principali protocolli di rete e applicativi
- installazione, configurazione, gestione e utilizzo di strumenti per la sicurezza di rete (Firewall Checkpoint e Linux-based, sistemi IDS/IPS, VPN, Network scanner...)
- installazione, configurazione e gestione di servizi per reti TCP/IP (web server, nameserver, server di posta, SMB/CIFS ecc.);
- configurazione e utilizzo di sistemi di virtualizzazione, principalmente basati su tecnologia VMware;
- personalizzazione e hardening di sistemi e kernel Linux

Vulnerability assessment

Dal 1995, fino al 2005 circa, nell'ambito delle attività security assessment, ho svolto vulnerability assessment sia interni che esterni (EVA), nei confronti di pubbliche amministrazioni, banche e industrie. L'attività è stata svolta anche in affiancamento a personale sia delle organizzazioni oggetto di verifica, che di aziende specializzate nella fornitura di servizi di sicurezza

Aspetti legali della sicurezza IT

Competenze in questa area comprendono:

- analisi dell'impatto della normativa vigente sulla gestione della sicurezza IT.
- implementazione di soluzioni di sicurezza per la conformità alle normative.

Formazione

Dal 1997 al 2014, collaborazioni a vario titolo con l'Università di Pisa per attività di didattica e ricerca del campo della sicurezza ICT;

Dal 1995, ho tenuto seminari e corsi a diversi livelli di approfondimento sui temi legati alla sicurezza dei sistemi informativi.

Open Source

Conoscenza approfondita delle problematiche legate allo sviluppo e all'utilizzo di software Open Source

Convegni

Relatore per diversi convegni su tematiche legate alla sicurezza ICT. Attività recenti o di particolare rilevanza comprendono:

“La sicurezza dei meccanismi di autenticazione SPID nel processo di autorizzazione per i Gestori di Identità” Security Summit, Roma 2016

Moderatore per la sessione: “L’impatto della Direttiva 263/agg.15 di Banca d’Italia sugli operatori del settore bancario”, Security Summit, Milano 2015

“New generation SOC”, Security Summit, Milano 2014

“La sicurezza a confronto con le esigenze di privacy e operatività” Convegno Sudsanità “Verso il nuovo Fascicolo Sanitario Elettronico. Nel segno dell’interoperabilità”, Catania, 2013

“Sicurezza del DNS”, Security Summit, Roma, 2012

“Le frodi interne”, Security Summit, Milano, 2010

“Evoluzione del Malware, Botnet e underground economy”, Security Summit, Roma, 2009

“Il Cigno Nero” Sessione di studio AIEA, 2009

“La micro, la piccola e la media impresa: mettere al sicuro il proprio business - Assintel/Clusit” Security Summit, Milano, 2009

“La virtualizzazione dell’infrastruttura di rete: potenzialità e rischi”. sessione di studio AIEA, 2006

“La sicurezza delle basi di dati”, Master “Governare i sistemi informativi: aspetti manageriali, giuridici e tecnologici”, Euros Consulting, 2003

Relatore per i Convegni Annuali dell’AIEA/ISACA (Associazione Italiana IT Auditors) negli anni 1995, 2000 e 2001.

Relatore sul tema: “La gestione in termini di sicurezza e tutela della privacy di sistemi per il commercio elettronico”, congresso Informatica e Riservatezza”, Pisa, settembre 1998; curatore degli Atti del Convegno

Principali pubblicazioni

AA.VV. “Rapporto Clusit sulla sicurezza ICT in Italia”, anni dal 2012 al 2016

AA.VV. “Innovazione Digitale a supporto dei Percorsi Diagnostico Terapeutici Assistenziali”, AISIS 2015

AA.VV. “MOBILE HEALTH: innovazione sostenibile per una sanità 2.0”, AISIS 2014

AA.VV. “Cartella clinica elettronica ospedaliera: indicazioni per un progetto sostenibile”, AISIS, 2012

AA.VV. “I primi 100 giorni del responsabile della sicurezza IT”, Oracle Community for Security, 2012

AA.VV. “Privacy nel cloud: le sfide della tecnologia e la tutela dei dati personali per un’azienda italiana”, Oracle Community for Security, 2012

“Unbounded impacts and risk mitigation in billing infrastructures”, Fabrizio Baiardi, Claudio Telmon and Daniele Sgandurra. In “Int. J. Risk Assessment and Management, Vol. 15, Nos. 2/3, 2011”

“Risk Modeling and Management of Billing Infrastructures.” Fabrizio Baiardi, Claudio Telmon and Daniele Sgandurra. In “Proceedings of the Third Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection”.

F. Baiardi, M. Pioli, S. Suin, C. Telmon: “Assessing the Risk of an Information Infrastructure through Security Dependencies”, International Journal of System of Systems Engineering (IJSSE) ISSN (Online): 1748-068X 2007

F. Baiardi, M. Pioli, S. Suin, C. Telmon: “Hierarchical Model Based Risk Management of Critical Infrastructures”, Special Session on Vulnerability, Reliability and Safety of Complex Networks and Critical Infrastructures, ESREL 2007, Giugno 2007

C. Telmon: “I rischi del Trusted Computing”, Quaderno CLUSIT n. 9, Febbraio 2007

F. Baiardi, S. Suin, C. Telmon: "Assessing the Risk of an Information Infrastructure through Security Dependencies" - First international workshop on critical information infrastructure security, Samo, Sett 2006

F. Baiardi, S. Suin, C. Telmon: "A Mathematical Framework to Assess the Security of an Information Infrastructure" - First italian workshop on privacy and security, Roma Giugno 2006

F. Baiardi, C. Telmon: "A Theoretical Model for the Average Impact of Attacks on Billing Infrastructures", LECTURE NOTES IN COMPUTER SCIENCE, num. 1, vol. 3685, pp. 298-310, 2005

F. Baiardi, F. Martinelli, L. Ricci, C. Telmon: "Constrained Finite State Automata for Risk Analysis and Assessment", NATO Advanced Research Workshop on Information Security and Assurance, vol. 1, pp. 898-1, Terouuan, Marocco 2005

AA.VV.: "Sicurezza Informatica", 2nd ed. Ed. McGraw-Hill, 2005 - Testo di preparazione per EUCIP IT Administrator - Modulo 5

AA.VV.: "Sicurezza Informatica", Ed. McGraw-Hill, 2003 - Testo di preparazione per ECDL IT Administrator - Modulo 5

ULTERIORI INFORMAZIONI

V. Ambriola, C. Telmon: "Protezione della rete di un'Organizzazione di Ricerca Non Profit: un case study", Congresso AICA '97 "Internet e oltre", settembre 1997.

Corso di formazione "La sicurezza e l'igiene nei luoghi di lavoro" per i datori di lavoro che assolvono ai compiti del servizio di prevenzione e protezione (art. 10 del D.L.g. n. 626/94 e succ.) a cura di Ascom - Confcommercio di Pisa - Novembre 1997

PATENTE Patente di Guida B

Autorizzo il trattamento dei dati personali sopra riportati ai sensi del decreto legislativo 196/2003