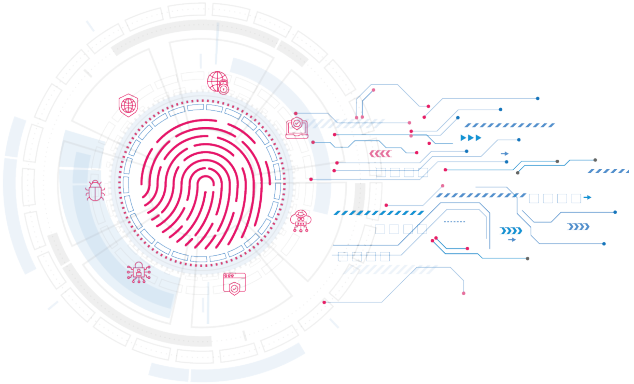
CYBER SECURITY 360 Summit



La nuova strategia italiana della cybersecurity
25 maggio 2022

Introduzione ai lavori e saluti di benvenuto
Alessandro Longo, *Direttore Responsabile, AgendaDigitale.eu e Cybersecurity360*

Keynote
Marcello Albergoni, *Gabinetto, Capo della Divisione affari giuridici, legislativi e legali Agenzia Cybersicurezza Nazionale*

Come garantire un'adeguata protezione attraverso la catena dei fornitori sia in ambito privato che pubblico e l'importante ruolo delle certificazioni
Alessandro Guarino, *Chairman CEN JTC 13 WG 5*

Tavola Rotonda – Come dimostrare l'adeguatezza delle proprie misure tecniche ed organizzative?
Il GDPR ha introdotto il principio di accountability: è diventato quindi necessario essere in grado di dimostrare di aver adottato tutte le misure di sicurezza necessarie ed opportune, oltre che di gestirle correttamente lungo tutta la filiera. Quale il ruolo delle certificazioni, in particolare quelle di cybersecurity, in questo scenario? Quali processi o strumenti possono supportare l'organizzazione nel dimostrare la propria adeguatezza ai propri clienti, alle Autorità o all'Organismo di certificazione stesso?

Partecipano:
Gianni Baroni, *CEO, Cyber Guru*

Cecilia Colasanti, *Data Protection Officer, ISTAT*

Nicola Fusco, *Security Operations Auditor, ArcaSafe*

Riccardo Giannetti, *Scheme Manager ISDP10003 & SGCMF10002, Training Manager, Lead auditor GDPR*

Fabio Guasconi, *Presidente BL4CKSWAN, Presidente, CT 510 "Sicurezza delle Informazioni" UNINFO e Membro del Comitato Direttivo, CLUSIT*

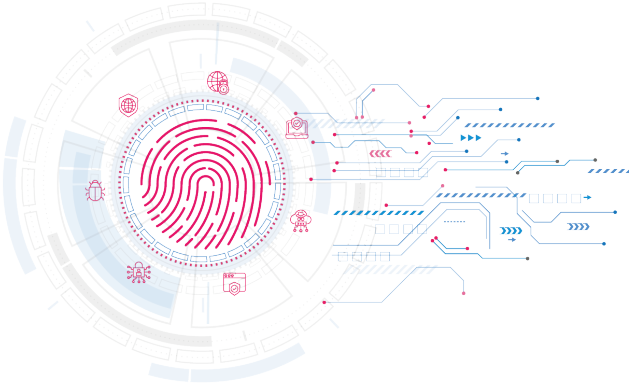
Rosario Imperiali, *Avvocato specializzato in normativa data protection italiana ed internazionale, House of Data*

Luca Piccinelli, *Chief Cybersecurity and Privacy Officer, Huawei Italia*

Francesco Pozzobon, *Chief Sales & Marketing Officer, Digital Attitude*

Modera: **Gabriele Faggioli,** *Presidente Clusit, CEO Digital360*

CYBER SECURITY 360 Summit



Data breach: ripercussioni economiche e finanziarie e impatto mediatico

Andrea Chittaro, *Senior Vice President Global Security & Cyber Defence Snam*

Tavola Rotonda – La gestione di un incidente: le nuove sfide

Sono in aumento i tentativi di attacco e sono in aumento i conseguenti incidenti e data breach. La capacità di identificare e gestire un incidente è diventato oggi un asset essenziale per ogni organizzazione. E', infatti, diventato necessario non solo identificare l'attacco, contrastarlo e mitigarne gli effetti, ma anche comunicare nel modo corretto con tutti gli stakeholder durante la gestione dello stesso.

Mentre, ad esempio, mentre il SOC collabora con le altre funzioni tecniche aziendali, diventa necessario veicolare le informazioni verso collaboratori, clienti, ove necessario o opportuno verso la Pubblica Autorità, i media, la compagnia assicuratrice, l'Autorità Garante per la protezione dei dati personali, lo CSIRT Italia, e qualsiasi ulteriore ente regolatore di riferimento per l'organizzazione vittima.

Quale il ruolo del CISO in questo scenario, in rapporto agli altri attori, quali gli strumenti e le accortezze da adottare al fine di mitigare l'impatto dell'incidente?

Partecipano:

Andrea Barchiesi, *Fondatore e CEO, Reputation Manager*

Daniela Bragante, *Data Protection Officer, Nexi*

Matteo Flora, CEO*, TheFool, socio co-fondatore, Centro Studi Hermes*

Antonio Forzieri, *EMEA Cyber Security Specialization and Advisory, Splunk*

Rocco Panetta, *Avvocato, Managing partner, Panetta & Associati, esperto di Internet e Privacy, Country Leader per l'Italia, IAPP International Association of Privacy Professionals*

Simone Ricci, *SE Manager Italia e Iberia, Forcepoint*

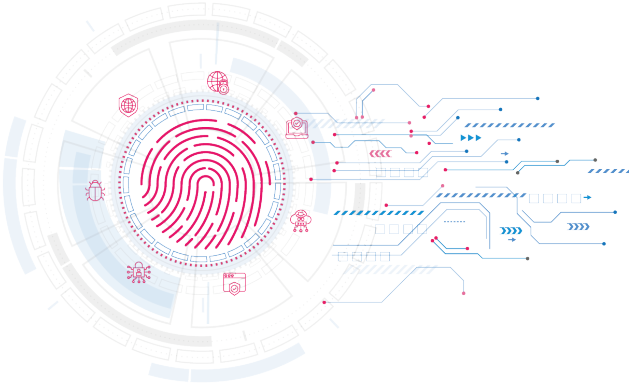
Modera: **Alessio Pennasilico**, *Information and Cyber Security advisor, Associazione informatici Professionisti*

Intervista – Il nodo sul trasferimento dei dati personali

Guido Scorza, *Componente del Collegio del Garante per la protezione dei dati personali*

Tavola Rotonda – Proteggere le informazioni anche in cloud

Il numero di aziende che ha adottato strategie cloud only o cloud first è in costante aumento. La valutazione di adeguatezza di un fornitore è già un processo complesso: quando ci si trova a dover valutare tutto il contesto multicloud dell'organizzazione le



variabili da analizzare aumentano. L'utilizzo, di servizi erogati o gestiti dall'esterno dell'UE pone, inoltre, la necessità di affrontare ulteriori rischi. Per questa ragione tecnologie di virtualizzazione, remotizzazione, crittografia, pseudonimizzazione, gestione degli accessi, zero trust diventano centrali per poter garantire la sicurezza dei dati affidati a fornitori terzi. Come affrontare il tema in modo strategico, in compliance con le norme cogenti? Quali sviluppi si prevedono per il futuro?

Partecipano:

Fabio Bassan, *Professore Ordinario di Diritto dell'Unione Europea, Università Roma Tre*

Luca Bolognini, *Avvocato, Presidente, Istituto Italiano per la Privacy e la Valorizzazione dei Dati (IIP)*

Alberto Da Pra, *Presale & Market Dev Mgr - Business Unit Cybersecurity, Corvallis*

Feliciano Intini, *Senior Cloud Compliance Specialist, Microsoft*

Franco Pizzetti, *Professore Emerito in Diritto Costituzionale, Università di Torino*

Giovanni Ziccardi, *Avvocato, Professore di "Informatica Giuridica", Università degli Studi di Milano*

Giusella Finocchiaro, *Professoressa Ordinaria di Diritto Privato e di Diritto di Internet, Università d Bologna, co-founder e partner DigitalMediaLaws*

Modera: **Anna Cataleta**, *Senior Partner P4I*

Riflessioni e saluti finali

Alessandro Longo, *Direttore Responsabile, AgendaDigitale.eu e Cybersecurity360*