Programma

8,30 - **Registrazione partecipanti**

8,45-9,00 - **Isabella Corradini,** *Professore di Psicologia sociale della Facoltà di Psicologia dell'Università degli Studi dell'Aquila e Presidente del Centro Ricerche Themis*

Introduzione Moderatore

9,00-9,20 - **Domenico Condello,** *Avvocato del Foro di Roma, Consigliere dell'Ordine degli Avvocati di Roma, Docente di Informatica Giuridica e Diritto dell'Informazione presso l'Università di Urbino e l'Università G. Marconi di Roma*

La dematerializzazione dell'identità digitale

9,20-9,40 - **Andrea Rigoni,** *Director General GC-SEC Global Cyber Security Center*

9,40-10,00 - Intevento a cura di **Walter Bruschi,** Amministratore Delegato **Card Protection Plan Italia**

Il furto di identità e gli italiani: tra percezione e prevenzione
La ricerca effettuata sui consumatori italiani da 25 a 60 anni sul furto di identità, evidenzia comportamenti e atteggiamenti contraddittori. Nonostante un'elevata percentuale di potenziale esposizione a furto di identità (circa metà del campione è potenzialmente esposto a furto di identità) e il 40% che si dichiara molto preoccupato da questo fenomeno, soprattutto per le difficoltà di rapida soluzione dello stesso e le potenziali problematiche legate a frodi o delitti, pochi e basilari appaiono i comportamenti e le tecniche difensive adottati per contrastare questi timori.Contraddittorio è anche l'atteggiamento nei confronti di Internet: da una parte viene considerato un "luogo" pericoloso, dal quale tutelarsi con appropriate difese, che in realtà sono blande o inesistenti, dall'altra è il "luogo" preferito dove effettuare operazioni potenzialmente rischiose, quali rilasciare proprie informazioni personali, eseguire transazioni economico-finanziarie e scambiare informazioni con "amici" dei quali sappiamo poco o nulla.In realtà ciò che sta emergendo, grazie a ricerche come la nostra, è che il cybercrime "non ha confini" e che la realtà supera a volte la fantasia. A questo punto, come prevenire e combattere il furto d'identità? Con la cultura, educando i consumatori, siano essi "on-line" o "off-line", per incrementare la percezione del fenomeno, per modificare i loro preconcetti e per spingerli a gestire i propri dati, specie quelli su Internet, con minore leggerezza

10,00-10,20 - **Domenico Vulpiani**, *Dirigente Generale Polizia di Stato. Consigliere del Ministero dell'Interno per la sicurezza informatica*

Un mercato fiorente: il furto d'identità digitali
C'è un mercato che non conosce crisi finanziaria, anzi è in continua crescita , si tratta del mercato nero delle informazioni, il c.d. black market. Il valore delle informazioni rubate nel 2009, secondo Il Symantec Intelligence Quarterly Report di aprile-giugno 2010, ammonterebbe ad un trilione di

dollari, i costi medi sostenuti da un'azienda compromessa si aggirerebbero da 5 milioni di euro fino a 23 milioni di euro. Tale dati trovano riscontro anche nelle denunce ricevute dalla Polizia Postale e delle Comunicazioni, nell'arco temporale 2008-2010. Si evidenzia, infatti, un trend crescente delle denunce per phishing (passate dalle 1754 nel 2008 alle 2148 del 2009 fino alle 2355 denunce di phishing consumato, a cui vanno ad aggiungersi le 694 denunce, per casi di phishing tentato, del 2010). I mezzi più utilizzati per la sottrazione di dati vanno dall'invio della nota "e-mail trappola" all'impiego di software ideati ad hoc, ma non va sottovalutata nemmeno l'importanza dell'insider. Queste sono solo alcune delle sfide quotidiane alla cyber security. Il futuro ne riserva ben altre, con l'avvento del cloud computing…

10,20-10,40 - **Andrea Lisi,** *Presidente A.N.O.R.C. Associazione Nazionale Responsabili Conservazione digitale dei documenti, Docente Informatica Giuridica S.S.P.L. , docente SDA Bocconi per la Document Management Academy, già docente dell'Università del Salento.*

10,40-11,00 - **Fausto Basile,** *Vice Capo Ufficio legislativo Ministro per la PA e per l'Innovazione*

Il documento informatico nel decreto correttivo al Codice dell'Amministrazione digitale - Elaborazione, sottoscrizione e trasmissione. Le firme elettroniche e la posta elettronica certificata

11,00-11,20 - Intevento a cura di **Claudio De Paoli -** Responsabile della Practice Sicurezza IT di **Almaviva** e **Mauro Costantini –** PreSales System Engineer di **RSA**

Contrasto delle frodi per il furto di identita' nella PA
Il furto di identità è un fenomeno in continua crescita nei servizi online. Tecniche come il phishing ed i Trojan sono usati in diverse industrie anche allo scopo di perpetrare frodi . Questa tipologia di fenomeno è oggi una concreta minaccia anche nella Pubblica Amministrazione. AlmavivA ed RSA hanno ideato un framework di servizi e soluzioni in grado di contrastare questi fenomeni nello specifico ambito dei processi della Pubblica Amministrazione. Il framework ideato dalle due aziende si basa sulle tecnologie di Web Fraud Detection di cui RSA è leader internazionale e sulla conoscenza dei processi e IT della Pubblica Amministrazione maturata da AlmavivA in oltre un decennio di collaborazione con la PA

11,20-11,40 - **Giovanni Manca,** *Esperto di digitalizzazione documentale nella PA e sicurezza ICT*

Le tematiche di sicurezza ICT nel nuovo CAD (dlgs 30/12/2010 n.235)
Le novità introdotte dal decreto legislativo 30 dicembre 2010, n. 235 hanno rilevanza nel settore della sicurezza ICT sia per la PA che per i privati. Importanti novità riguardano la disciplina delle firme elettroniche, della conservazione digitale, della continuità operativa e della sicurezza dei dati nella PA. Nell'intervento vengono evidenziate sinteticamente tali novità ipotizzando, ove opportuno, lo scenario che andranno a configurare le regole tecniche in corso di emanazione

11,40-12,00 - Intevento a cura di **Michele Mantovani,** Country Manager **EMC Information Intelligence Group**

Dal protocollo informatico alla completa dematerializzazione: la sfida della PA Digitale
Il percorso verso le amministrazioni digitali e interconnesse è stato avviato in Italia con l'adozione di soluzioni di protocollo informatico. A questo primo passo devono seguire interventi mirati alla ottimizzazione dei procedimenti, alla gestione automatizzata delle pratiche, e alla gestione totalmente elettronica delle informazioni in modalità sicura e convidisa. I principali benefici derivanti da una completa dematerializzazione sono rappresentati dalla riduzione dei rischi (legati al

supporto cartaceo) di perdita o diffusione non autorizzata di dati importanti e dalla opportunità di condivisione e valorizzazione delle informazioni all'interno dei singoli enti e tra enti e cittadini

12,00-12,20 - **Gabriele Cicognani,** *Responsabile del Cert-Spc di DigitPA*

Cyber(in)security
L'intervento illustrerà lo scenario, le tendenze delle principali minacce registrate in danno all'utenza della Rete, con particolare riferimento a recenti casi di furti di identità digitale ed all'efficacia dell'azione di prevenzione e contrasto posta in essere nel nostro paese per contrastare il fenomeno del cybercrime nelle sue diverse modalità attuative.

12,20-12,40 - Intervento a cura **Andrea Orsucci**, Amministratore di **Avangate**

A causa delle minacce informatiche ogni anno le aziende perdono almeno 500 EUR per dipendente: come coniugare sicurezza, semplicità e risparmio.
Le moderne organizzazioni, private e pubbliche, sono oggetto di attacchi informatici da più fronti. Tali attacchi provocano perdite di informazioni, tempo e risorse. Panoramica dei casi seguiti, protezione locale e periferica contro virus e spam attraverso le soluzioni proposte da Avangate e basate sui prodotti AVG ed AntispamEurope Analisi di casi reali, pubblici e privati, con particolare attenzione alla necessità di diversi livelli di protezione

12,40-13,00 - **Elio Molteni,** *Presidente AIPSI*

Le nuove Frontiere dell'Identity and Access Management
In un mondo in cui i furti di identità sono sempre più attrazione dei malfattori, non basta più definire le identità ed assegnarne le corrette autorizzazioni. Deve essere perseguito il principio che "le informazioni devono essere usate nel giusto modo dagli individui autorizzati in accordo al proprio ruolo e ai privilegi assegnati". Se ci fermiamo ai soli diritti di accesso, va da sé che un utente autorizzato a visualizzare certe informazioni confidenziali possa a sua volta trasferirle all'esterno tramite canali ormai di uso quotidiano, memory card, email, internet. E' quindi indispensabile per garantire una adeguata mitigazione dei rischi, aggiungere al "Chi fa cosa" anche una dimensione rappresentata dall'uso vero e proprio di queste informazioni.

13,00-13,20 - **Raoul Chiesa**, *@ Mediaservice.net, Founder, Senior Advisor, Cybercrime Issues & Strategic Alliances, UNICRI (United Nations Interregional Crime & Justice Research Institute)*

Cybercrime, CyberWar, Information Warfare: what's this all about? New Rules for a new world
Questa presentazione porterà il pubblico in un mondo inusuale, dove i Signori del Crimine di oggi, insieme a Governi e Forze Armate, stanno iniziando qualcosa mai visto prima, seppur operando da due punti di vista e scenari completamente differenti. Verranno mostrate fotografie ed evidenze, raccolte lavorando in questi nuovi contesti.

13,20-14,20 - **LUNCH**

14,20-14,30 - **Roberto Setola**, *Docente e Direttore del Laboratorio Sistemi Complessi e Sicurezza Università CAMPUS Bio-Medico di Roma*

Introduzione moderatore

14,30-14,50 - Intervento a cura di **Antonio Marsico,** Responsabile Soluzioni di Sicurezza **Hewlett-Packard**

Trasformazioni sociali e mondo digitale: Sicurezza e Privacy
La facilità di duplicazione e trasmissione delle informazioni nell'era digitale sollevano questioni importanti e introducono un cambiamento di atteggiamento, per cercare di trovare il giusto equilibrio tra libera espressione, accesso a servizi, sicurezza e privacy. La proposta HP per il processo di definizione dei requisiti di Sicurezza e Privacy e per la realizzazione di un Security Model

14,50-15,10 - Intervento a cura di **Lucilla Mancini,** Responsabile della struttura consulenza di **Business-e**

DLP: uno strumento per la compliance
La conformità a norme e standard richiede, tra l'altro, implementazione di contromisure atte a impedire la violazione delle stesse. Nuove soluzioni e strumenti supportano le aziende in questo; infatti partendo dall'analisi dei rischi consentono di individuare i dati da proteggere e la loro corretta gestione attraverso soluzioni tecnologiche ed organizzative che recepiscono al meglio i dettami della legge

15,10-15,30 **- Massimo Penco,** *Presidente Associazione Cittadini di Internet, Membro del Antiphishing Working Group, Vice presidente Gruppo Comodo*

L'identità digitale: un problema irrisolto
Il problema del secolo dove gli studiosi di tutto il mondo non trovano soluzione definitiva rischia di divenire il "nuovo mostro" di Internet della comunicazione in genere delle intercettazioni e non solo. Un attenta analisi sul teorema delle "4 P" indica le strade da non seguire nella attività forense che sempre più si sta orientando verso prove scientifiche a volte senza un filo logico.

15,30-15,50 - Intervento a cura di **Luca Collacciani,** Major Account Executive di **Akamai**

Essere nel cloud significa essere al sicuro?
La nuova tendenza del cloud computing pone nuovi interrogativi in termini di sicurezza informatica. Avere una architettura cloud-based significa essere al sicuro rispetto ad attacchi informatici? Sicurezza non è solo riservatezza delle informazioni, è anche e soprattutto disponibilità e affidabilità del servizio e integrità dei dati aziendali. Akamai è il motore su cui si appoggiano i maggiori attori media ed e-commerce mondiali. Attraverso la propria rete distribuita di oltre 80.000 server nel mondo, Akamai fornisce servizi di Content Delivery Network, accelerazione applicativa e una suite completa di feature di sicurezza finalizzate alla protezione dei contenuti e delle informazioni aziendali.

15,50-16,10 - **Fabio Di Resta**, *Specialista legale privacy e diritto delle nuove tecnologie – LLM – ISO 27001 ICT Security auditor – Studio legale Di Resta*

Il quadro normativo in tema di identità digitale e prospettive future
La tutela dell'identità digitale è un tema prioritario, nel settore bancario ma anche il altri settori. Tra le diverso forme in cui può essere realizzato, il fenomeno del phishing è forse quello più conosciuto ed è entrato a far parte nel linguaggio comune. Nonostante vi siano numerosi gli strumenti normativi ed investigativi diretti a tutelare il patrimonio delle vittime di atti criminali, in contesti complicati connessi alle forme di criminalità perpetrati tramite internet gli strumenti messi in campo risultano purtroppo limitati e scarsamente efficaci. Il furto di identità commesso tramite internet

coinvolge spesso aspetti internazionali, i quali necessitano non solo di strumenti normativi efficaci ma di una cooperazione internazionale a diversi livelli che tenga il passo con il progresso tecnologico

16,10-16,30 - **Matteo Lucchetti,** *Senior Research Analyst ABI Lab*

La gestione sicura dell'identità elettronica nel settore bancario italiano - Opportunità e prospettive di evoluzione
L'intervento affronta il tema della gestione sicura dell'identità elettronica in banca sotto il profilo delle iniziative che si prevede possano interessare l'intero settore nel breve-medio periodo. Dopo aver inquadrato il fenomeno della sicurezza delle identità elettroniche in banca, descrivendo lo scenario delle minacce e delle principali contromisure adottate, sarà illustrato il percorso intrapreso dal sistema bancario, anche alla luce di alcuni recenti sviluppi del quadro regolamentare, tra cui l'avvento della PSD, l'integrazione dei canali di erogazione dei servizi di banche e PA e le evoluzioni delle azioni antifrode

16.30-16.50 - **Andrea Biasiol**, *Università Campus Bio-Medico*

Identità1 digitale e suo utilizzo in ambito ospedaliero: alcuni esempi applicativi presso l'Università Campus-Biomedico di Roma

16.50-18.00 - **Raoul Chiesa e Isabella Corradini**

Intervento tecnico-psicologico su ricerca UNICRI (United Nations Interregional Crime & Justice Research Institute sul furto della identità digitale.
L’intervento intende sottolineare l’analisi integrata dei fenomeni legati al cyber crime e alla sicurezza delle informazioni. L’analisi tecnica associata a quella psicologica permette di comprendere la reale portata dei fenomeni criminali legati alla tecnologia, il profilo degli autori di reato e il loro modus operandi. Come si sta evolvendo la criminalità informatica nel contesto attuale? Cosa caratterizza gli hacker oggi? Qual e' il confine tra hacking e cybercriminalita' ? Che cosa è consigliabile fare in termini di prevenzione? Ancora una volta si sottolinea l’importanza di integrare l’approccio tecnologico con quello umano per ottenere risultati efficaci nella prevenzione.