PROGRAMMA CONFERENZE 2018

CONFERENZA DI APERTURA

LE MINACCE DEL MONDO MODERNO: L'ATTUALE SITUAZIONE DELLA SICUREZZA AZIENDALE

Garantire un ambiente sicuro nel rispetto della propria cultura è oggi la sfida di tutti i professionisti della sicurezza.
Una panoramica degli incidenti più recenti e dei trend in corso ci guiderà verso la discussione delle criticità che i Direttori della Sicurezza devono fronteggiare.
Tra gli argomenti in discussione:

- L'anatomia del programma di sicurezza aziendale
- Ottenere il coinvolgimento della "C-suite" per garantire il successo del tuo programma di sicurezza
- Come creare un team di valutazione delle minacce per rispondere alle violenze sul posto di lavoro, alle risoluzioni conflittuali del rapporto di lavoro, ai furti interni ed esterni, alle frodi
- Critical Incident Response e piani di continuità operativa
- Protezione del brand

Patrick M. Conley, former Special Agent at FBI

WORKSHOP TEMATICHE DI SETTORE

IL PROCESSO DI RISK MANAGEMENT PER IL GOVERNO DEI RISCHI: VIRTÙ DI POCHI O NECESSITÀ PER TUTTI?

Partiamo da questo assunto: "Il Risk Management è la tecnica di gestione dei rischi d'impresa che tende a salvaguardare attraverso l'uso di strumenti di varia natura (prevenzione, protezione, assicurazione, etc…) e nelle migliori condizioni di costo, il patrimonio dell'impresa contro le perdite che possono colpirla nell'esercizio delle proprie attività".
Tuttavia, malgrado l'esplosione delle conoscenze, il trattamento del rischio non è spesso pianificato e prepariamo una risposta agli eventi solo dopo che essi sono accaduti e non sulla scorta di un progetto elaborato in anticipo, pur sapendo che le conseguenze di una scarsa o mancata pianificazione e preparazione a trattare il rischio possono essere catastrofiche.
E' per questo che, invece di continuare a trattare i diversi rischi in modo separato, bisogna attivare un lavoro di squadra che, con il coordinamento e il supporto del Risk manager, punti a mettere insieme le diverse competenze specialistiche come lo è quella del Security manager.
Il Risk Management ovviamente non è la panacea per risolvere tutti i problemi dell'azienda, ma l'organizzazione che riconoscerà la validità dei concetti che lo ispirano, non soltanto migliorerà i propri risultati, ma opererà anche su un nuovo terreno e in anticipo sui concorrenti.

Mauro A. Del Pup, Risk Manager Senior, Phoenix Informatica Bancaria SpA

LA SICUREZZA NELLE ORGANIZZAZIONI COMPLESSE

La complessità è insita nelle organizzazioni ma anche negli eventi.
Quali sono le best practice per la gestione di complessità relative alla sicurezza?
Quali sono i problemi, le difficoltà e le soluzioni necessarie per assicurare la protezione di una organizzazione medio/grande o di un evento complesso?
Quali sono le sfide che dobbiamo affrontare e le esperienze che ci aiutano?
La sessione sarà centrata su questi temi per favorire un dialogo aperto sulle risposte a queste domande

Luisa Franchina, Presidente AIIC associazione italiana esperti infrastrutture critiche

IL POSIZIONAMENTO DELLA SICUREZZA NELLA ORGANIZZAZIONE E NELLA GOVERNANCE AZIENDALE

Quale è il giusto collocamento della Sicurezza in una organizzazione aziendale? Safety e Security, sono due facce della stessa medaglia?
Sempre più spesso si parla di questo tema che, a volte, vede soluzioni o ipotesi fantasiose, a volte ragioni più o meno valide per ipotizzarne il collocamento a riporto del direttore HR, dell'AD o del Presidente. Ma vediamo anche casi in cui la sicurezza sta in area tecnica o addirittura commerciale.
Certo, tanto dipende dall'entità dell'Azienda di cui si parla ma, oggi, il quadro normativo delinea una serie di responsabilità in capo ai vari soggetti, che non è più possibile seguire la fantasia o le ragioni più o meno di parte.
Se Safety e Security non possono non prescindere da un sistema di deleghe vero ed effettivo, all'interno del quale le responsabilità sono ben identificate, la collocazione di questo Manager diventa chiara, semplice e logica: deve riportare direttamente al delegante o comunque al vertice dell'Azienda.

Stefano Bargellini, Executive Advisor Safety, Security and Property - Commendatore al Merito della Repubblica Italiana

IL FATTORE UMANO: LA COMPLESSITÀ DELLA CHIAVE DEL SUCCESSO

I modelli organizzativi di impostazione anglosassone tendono a creare strutture che operino a prescindere dalla qualità dell'uomo che vi interviene: è un approccio corretto? L'uomo è un elemento di complessità che incrementa o riduce i fattori di rischio? L'uomo è e rimane il protagonista vero delle opportunità come delle incognite. E' possibile costruire modelli di azione e di tutela che tengano conto del fattore umano nelle sue diverse valenze?

Manuel Di Casoli, Direttore Affari Legali e Security, Mediamarket S.p.A.

COMUNICAZIONE IN SITUAZIONI DI CRISI: TEMPI, METODI, SUGGERIMENTI E CASE-HISTORY

Le recenti vicende del Diselgate Volskwagen e del Datagate Facebook hanno messo ancora una volta in chiara evidenza come nei momenti di crisi e di potenziale pregiudizio reputazionale il ruolo della comunicazione diventi strategico e dirimente. Chi si occupa di sicurezza potrebbe sentirsi troppo occupato su altri fronti per potersi preoccupare anche di questi aspetti, ma non è così: una comunicazione mal gestita, sia verso i mass-media che diretta verso l'opinione pubblica, può recare grave pregiudizio - anche patrimoniale - all'azienda, e saper comunicare al meglio - e soprattutto sapere cosa comunicare, e prepararsi a farlo con ampio anticipo - è fondamentale.
Per questo abbiamo invitato Luca Poma, esperto di Crisis communication e crisis management, a tenere questa sessione. Con l'aiuto di esempi pratici e analisi di casi noti, ci aiuterà a decifrare i linguaggi utilizzati e gli effetti provocati nella gestione di crisi, e ci permetterà di trarne un utile decalogo che potrà aiutare i manager della sicurezza a sentirsi "più sicuri" anche sul fronte della comunicazione.

Luca Poma, Professore in Reputation Management all'Università LUMSA di Roma e specialista in Crisis Communication

LA TRAVEL SECURITY: LA PROTEZIONE DEL PERSONALE IN TRASFERTA

Il concetto di Duty of Care ed un forte risveglio di responsabilità da parte delle aziende verso il proprio personale (più ancora delle minacce terroristiche) hanno fatto sì che il tema della Travel Security sia entrato pesantemente nell'agenda di ogni Security Manager.
Si tratta però di un tema molto complesso e che non si può inventare dall'oggi al domani; nel dettaglio parleremo di:

- L'importanza (ampiamente tralasciata) di sapere dove sono i nostri dipendenti: il collegamento fra Security e le Travel Agency
- I Sw di localizzazione del personale e le mappe del rischio
- La Travel Security non è quello che facciamo sul campo (scorte, auto blindate, etc.) ma la preparazione del viaggio
- Gli strumenti tecnologici per le aree ad alto rischio
- L'importanza della formazione pre-partenza

- I questionari pre-partenza (Security Clearance Form) e le relative approvazioni
- I protocolli MedEvac
- I sistemi informativi mail, sms, telefono sulle situazioni di dettaglio ed in evoluzione
- I fornitori internazionali di servizi di security on-site

Matteo Tassoni, Country Security&Crisis Manager (Italy, Balkans, Greece & Israel), ABB SpA

LA CYBER SECURITY AZIENDALE E LE NUOVE FRONTIERE DELLA SICUREZZA

I sistemi informatici e di sicurezza presenti nel marcato ad oggi, non possono autonomamente garantire una completa protezione contro le attuali minacce e contro i Cyber Criminali, allo stesso modo non basta delegare il lavoro di controllo ai tecnici del settore IT.
E' pertanto necessario sviluppare un piano dedicato ad ogni tipologia di azienda effettuando formazione Cyber a tutte le cariche Aziendali, dal CEO all'ultimo stagista, installazione e configurazione di dispositivi sicuri mediante Best Practice.
Ricordiamo che "la Sicurezza NON è un prodotto ma un processo".
Durante questo intervento analizzeremo come gestire questo processo e cosa comporta per i responsabili della sicurezza, i tecnici ed altre cariche aziendali.
Infine faremo un breve accenno alla nuova normativa GDPR e cosa comporta adempiere ad essa per evitare spiacevoli sanzioni.

Pawel 'okno' Zorzan Urban, Cyber Security Manager, Hacker, Penetration Tester – Undisclosed

IL CRISIS MANAGEMENT vs L'EMERGENCY PLAN vs BUSINESS CONTINUITY PLAN

Tutt'oggi in Italia (ma non solo) i tre argomenti sono spesso gestiti in maniera fortemente separata e, spessissimo, da funzioni diverse:

- Crisis Management: Security
- Emergency Plan: HSE
- BCP: Operativo

Questo ha generato un forte scollamento di tre temi che invece sono fortemente collegati.
Affronteremo l'esperienza pilota di ABB nell'unire questi tre temi e nella creazione dei team dedicati.

Matteo Tassoni, Country Security&Crisis Manager (Italy, Balkans, Greece & Israel), ABB SpA

WORKSHOP TEMATICHE MANAGERIALI
PROVE TECNICHE DI NEGOZIAZIONE
Gestire il conflitto come generatore di valore

Il conflitto è quotidiano, è lì, dalla notte dei tempi nella storia dell'uomo e nel nostro quotidiano. Troppe volte confuso con la guerra, il conflitto è considerato come qualche cosa di negativo.
Una vita senza conflitto è come stare con qualcuno che la pensa sempre come te: una vita forse calma, ma sterile. È comunque utopica.
È attribuita a George Bernard Show questa frase "Se tu hai una mela e io ho una mela e ci scambiamo le nostre mele allora tu ed io avremo ancora una mela a testa. Ma se tu hai un'idea e io ho un'idea e ci scambiamo queste idee, allora ciascuno di noi avrà due idee".

Il conflitto va però gestito. Per farlo bisogna riconoscerlo e accettarlo prima, e poi tradurlo in un'opportunità.
Per questo servono abilità relazionali, che fanno capo alla capacità di negoziare.

Alessandra Colonna ci accompagnerà in un breve ma intenso viaggio dentro la negoziazione e risponderà a questa domanda: "Come creare da un dissenso un accordo di valore e un assetto relazionale sano?".

Alessandra Colonna, Managing Partner di Bridge Partners®, prima e unica società italiana specializzata in negoziazione.

LEADERSHIP: UN GIOCO D'EQUILIBRIO

Dai tempi antichi all'interno del gruppo nasceva il leader naturale. In passato era chi dimostrava la personalità più forte o chi magari era più determinato degli altri: questa persona serviva per mediare la competizione interna oltre a proteggere il gruppo contro il male (altri tribù o predatori). La leadership quindi diventò una risorsa necessaria, quasi fondamentale per la sopravvivenza e l'efficacia del gruppo. Quali sono le competenze che servono oggi per assicurare la produttività del team? E quanto peso ha un bravo leader sui risultati aziendali? Il 58% dei collaboratori dicono che la propria produttività soffre di fronte a un pessimo leader. Trovare il giusto equilibrio tra stimolare la motivazione e pretendere la performance è sempre una sfida. Ma se ognuno gioca il suo ruolo nel modo corretto, finisce che la motivazione spinge la performance... e i risultati possono solo arrivare!

Katherina Tsalikis, Executive Coach & HR Consultant

PER TROVARE LA SOLUZIONE DIMENTICA IL PROBLEMA

Dall'analisi del problema al focus sulla soluzione. L'approccio tradizionale al problem solving, prevede che davanti ad un problema si inizi sempre con un'accurata e spesso prolungata analisi della situazione. L'approccio focalizzato sulle soluzioni, soluzione focus, tende invece a concentrare tutta l'attenzione sulla visione, sulle risorse, sui compiti, sugli
obiettivi. E' un metodo di lavoro che si basa sul concetto di cambiamento (se continuiamo a fare una cosa come è stata sempre fatta l'esito sarà sempre il medesimo) e che enfatizza i successi, concentrandosi su ciò che funziona. "Non occorre sapere come funziona la serratura per aprire la porta, basta avere la chiave" il tema verrà trattato attraverso la metodologia Esperienziale, coinvolgendo i partecipanti in attività pratiche intervallate da momenti di riflessione e pillole teoriche.

Cecilia Venezia Psicologa, formatrice e coach

EXHIBITOR INSIGHTS

Videosorveglianza intelligente e impatto privacy

I nuovi sistemi di videosorveglianza permettono ciò che mai avremmo osato pensare… Come usarli nel pieno rispetto della normativa vigente?

A CURA DI HIKVISION

PROGRAMMA CONFERENZE 2018

CONFERENZA DI APERTURA

LO SCENARIO DELLE CYBER MINACCE: I TREND E L'UTILIZZO DEI PRINCIPI DI RISK MANAGEMENT PER DIFENDERE LE RETI

Lo scenario delle minacce in ambito cyber è un ambiente in continua trasformazione.

Gli attori delle minacce si avvantaggiano sia delle vulnerabilità tecniche che di quelle umane attraverso il social engineering.

L'intervento esaminerà l'attuale scenario delle minacce, visto attraverso la lente dell'FBI,
e offrirà osservazioni su pratiche di risk management e sullo sviluppo di programmi di information security, per aiutare i manager a rendere sicure le reti e a informare i vertici dell'azienda dei possibili rischi.

Malcolm K. Palmore CISM, CISSP - Information Security / Risk Management Executive - FBI San Francisco - Cyber Branch
M. K. Palmore serves as the leader of the San Francisco FBI - Cyber Security Branch. His responsibilities include the strategic and operational management of several teams of cyber intrusion investigators, computer scientists,

analysts and digital forensics personnel charged with conducting investigations of cyber threat actors in both the criminal and national security intrusion realms.
Mr. Palmore's leadership and investigative experiences include: Cyber Security, Crisis Management/Response, Internal Risk-Management Advisory and Counter-Terrorism matters.
Mr. Palmore entered on duty with the FBI in 1997. His assignments, in addition to San Francisco, have included FBIHQ (Washington, D.C.), Sacramento, Los Angeles and several overseas engagements. In addition to his operational duties, Mr. Palmore writes extensively on the subject of leadership and has been interviewed by several outlets on the subjects of Information Security and Cyber Security Awareness.
Mr. Palmore's certifications include the ISACA – CISM, ISC2 – CISSP and the Carnegie Mellon University CISO Certificate. He earned a B.S. from the United States Naval Academy and a MBA from Pepperdine University. Prior to the FBI, Mr. Palmore served as a commissioned officer in the United States Marine Corps.

CONFERENZA SERALE

PROSPETTIVE DELLA DIFESA PER LA SICUREZZA CIBERNETICA

L'intervento verterà sull'evoluzione dell'organizzazione Difesa nel dominio cyber. Nello specifico si fornirà un cenno al quadro normativo di riferimento da cui discende quanto realizzato dalla Difesa nel settore della Cyber Defence e si illustrerà l'organizzazione preposta per l'assolvimento dei compiti discendenti; saranno illustrati gli aspetti primari che stanno portando verso un'evoluzione organizzativa tesa al completamento della capacità di Cyber Defence e al raggiungimento di una piena capacità anche nelle Cyber Operations, attraverso la costituzione del Comando Interforze per le Operazioni Cibernetiche, definendo le future esigenze formative della Difesa, organizzative e infostrutturali. L'intervento si concluderà con delle considerazioni finali e degli elementi di riflessione generali.

Francesco Vestito – Generale di Brigata Aerea – Capo del CIOC Comando Interforze Operazioni Cibernetiche
Il Generale di Brigata Aerea Francesco Vestito è Capo del Comando Interforze per le Operazioni Cibernetiche, ente alle dipendenze del Sottocapo di Stato Maggiore di SMD, responsabile per la Pianificazione e Condotta di Operazioni Cibernetiche Militari, lo sviluppo dei Concetti e della Dottrina Interforze di settore in campo nazionale e internazionale.
Proviene dal Corso EOLO IV dell'Accademia Aeronautica ed ha conseguito il brevetto di Pilota Militare al ENJJPT nella Air Force Base di Sheppard (Texas, USA) con la Classe 90-06. Dopo il Transition Course sul TORNADO al TTTE in Cottesmore (UK), è stato assegnato al 36° Stormo di Gioia del Colle (BA) dove ha acquisito la Combat Readiness nel ruolo Bombardiere.
Ha al suo attivo oltre 3000 ore di volo sul Tornado IDS, operando nei Teatri Operativi nei Balcani, in Libia e Afghanistan. Nell'assolvere gli obblighi di Comando ha ricoperto l'incarico di Comandante del 156° Gruppo, della Joint Air Task Force per l'Operazione ISAF in Herat (Afghanistan) e del 6° Stormo di Ghedi.
Tra le varie qualifiche, si menzionano quelle di Tornado Instructor Pilot, Weapon Instructor e Crew Resource Manager Facilitator. Ha anche frequentato il Tactical Leadership Program a Gilze Rijan (NLD), il Joint Combined Warfighting Course a Norfolk (Virginia, USA), il Safety Management System Course ad Amsterdam (NLD) ed il Defense Resource Management Course a Monterey (California, USA). Tra gli incarichi precedenti, quello di Capo

del 1° e 5° Ufficio presso SMA 3° Reparto e Capo Ufficio Sperimentazione presso il Centro Innovazione della Difesa, per poi assumere l'incarico di Direttore dello stesso Centro.
Ha conseguito il Master in Studi Strategici presso l'Air War College in Montgomery (Alabama, USA).

SEMINARI

COME DEFINIRE IL CYBER-BUDGET (E PERCHÉ)

Attualmente i budget dedicati alla IT Security (per non parlare della Cyber Security, per la quale i budget sostanzialmente ancora non esistono) sono per lo più derivati dal budget IT.
Nel corso del seminario dimostriamo che questo approccio non è più sostenibile, anzi è controproducente, dato il livello raggiunto dalle minacce (che rappresentano ormai un pericolo esistenziale per le nostre organizzazioni), e proponiamo un modello logico-pratico di definizione del cyber-budget commisurato al contesto attuale.

Andrea Zapparoli Manzoni
Si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking.
E' stato membro dell'Osservatorio per la Sicurezza Nazionale (OSN) nel 2011-12 e del Consiglio Direttivo di Assintel dal 2012 al 2016, coordinandone il GdL Cyber Security.
Dal 2012 è membro del Consiglio Direttivo di Clusit, e Board Advisor del Center for Strategic Cyberspace + Security Science (CSCSS) di Londra.
Per oltre 10 anni è stato Presidente de iDialoghi, società milanese dedicata alla formazione ed alla consulenza in ambito ICT Security.
Nel gennaio 2015 ha assunto il ruolo di Head of Cyber Security Services della divisione Information Risk Management di KPMG Advisory.
Dal giugno 2017 è Managing Director di un centro di ricerca internazionale in materia di Cyber Defense.
E' spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero.
Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security.
Fin dalla prima edizione (2011) del "Rapporto Clusit sulla Sicurezza ICT in Italia", realizza la sezione relativa all'analisi dei principali attacchi a livello internazionale, ed alle tendenze per il futuro.

GESTIRE LA SICUREZZA AI TEMPI DEL GDPR

A quasi un mese dalla definitiva applicazione del Regolamento europeo in materia di protezione dei dati personali, il seminario si pone l'obiettivo di analizzare lo stato dell'arte con particolare riferimento alle "adeguate" misure di sicurezza previste dal legislatore comunitario. Verranno esaminate le linee guida emesse in materia dalle principali Autorità europee e le recenti attività di armonizzazione effettuate dal Garante Privacy italiano. Si affronteranno, tra le altre, tematiche strategiche legate all'accountability del titolare del trattamento e al rapporto tra l'approccio basato sul rischio e l'obbligo di notifica delle violazioni di dati personali (c.d. data breach). Quali azioni dovrebbero già essere operative nelle

organizzazioni? Quali invece potrebbero essere le attività da pianificare e indirizzare nel medio-lungo periodo? Durante il seminario si forniranno una serie di spunti derivanti dall'esperienza maturata sul campo al fine indirizzare i futuri interventi di Cyber Security muovendosi cum grano salis all'interno di un framework normativo complesso con un elevato impatto sui sistemi informativi.

Alessandro Rodolfi, *Alessandro Rodolfi (1975), giurista appassionato di nuove tecnologie applicate a contesti insicuri o problematici, è cultore della materia alle cattedre di Informatica e Informatica giuridica avanzata presso la facoltà di Giurisprudenza dell'Università degli Studi di Milano. E' docente in diversi corsi di perfezionamento e master di specializzazione relativi alla protezione dei dati e membro della commissione d'esame per un noto ente di certificazione ai fini del rilascio di certificazioni di profili professionali concernenti il ruolo di DPO in conformità alla norma UNI 11697:2017.*

CYBER TERRORISM: IPOTESI SBAGLIATE E FATTI VERI + CIÒ CHE SPERO NON ACCADA MAI!

Questa presentazione inizierà con una definizione provvisoria del termine "Cyber Terrorismo", poi ci concentreremo su quelle supposizioni sbagliate che ci facciamo spesso leggendo le notizie divulgate dai mezzi di informazione.
Lo speaker analizzerà l'argomento con fatti reali e veri, dirigendosi così verso il vero "nucleo" del suo discorso: cosa i (cyber) terroristi non hanno (ancora) fatto, o meglio "cosa speriamo davvero che non accada mai".
La presentazione terminerà con la prospettiva di un "possibile attacco terroristico informatico", in modo che tutti noi possiamo effettivamente capire quanto le problematiche inerenti ICT e Info Sec influenzino e influiscano sulla nostra "vita reale" e sul mondo di oggi.

Raoul Chiesa
Raoul "Nobody" Chiesa dopo essere stato tra i primi hacker italiani a cavallo tra gli anni'80 e '90 decide di muoversi verso l'Information Security professionale e fonda una delle prime società italiane di «security advisory» vendor-neutral.
In vent'anni di carriera «Nobody» è arrivato a ricoprire importanti ruoli presso diverse Associazioni, Enti e security community, sia nazionali che internazionali: CLUSIT, ISECOM e 'OWASP Italian Chapter, è stato per tre anni tra i coordinatori del Gruppo di Lavoro «Cyber World» presso il CASD/OSN (Centro Alti Studi per la Difesa / Osservatorio per la Sicurezza Nazionale) e membro dell'Osservatorio Italiano Sicurezza & Privacy (AIP/OPSI); nel 2013 viene scelto come coordinatore per l'Italia del capitolo europeo di APWG.EU (Anti-Phishing Working Group) e nel 2015 viene eletto nel Consiglio Direttivo dell'AIIC (Associazione Italiana esperti di Infrastrutture Critiche).
A livello istituzionale, dal 2003 ha iniziato la sua collaborazione con l'agenzia delle Nazioni Unite "UNICRI" come ideatore del progetto "HPP", l'Hackers Profiling Project, noto in tutto il mondo; oggi è "Special Advisor on Cybercrime Issues and Hackers Profiling".
Nei bienni 2010-12 e 2013-15 è nel PSG (Permanent Stakeholders Group) tramite chiamata «ad personam» dal Direttore della stessa agenzia ENISA, la European Union Network & Information Security Agency.
Nel 2015 Raoul diviene membro del prestigioso Roster of Experts presso l'ITU (International Telecommunication Union, Nazioni Unite) di Ginevra.
E' autore di numerose pubblicazioni, cartacee ed on-line, di settore e generaliste, sia in Italia che ed è ospite in trasmissioni nazionali ed estere sin dal 1996.

BITCOIN, BLOCKCHAIN & CYBER-SECURITY

Il termine "blockchain" è attualmente usato (ed abusato) come una parola magica per suscitare facili entusiasmi: una "buzz-word" a tutti gli effetti. In questo workshop verranno analizzate le caratteristiche fondamentali e le potenziali implicazioni che si nascondono, spesso in modo confuso, dietro al termine, per andare oltre l'"hype" mediatico e verso la sostanza, tramite un inquadramento dettagliato delle tecnologie "blockchain" (e "blockchain-inspired"), del protocollo Bitcoin, delle cosiddette "crypto-currency", con particolare attenzione alla sovrapposizione e all'interazione di questi temi con quelli tipici dell'industria Cyber-sec. Verranno sfidati alcuni luoghi comuni, riportando l'attenzione su use-cases realistici e possibili applicazioni industriali e di mercato.

Giacomo Zucco
dopo una laurea in Fisica con indirizzo teorico nel 2009, ha lavorato per alcuni anni come Technology Consultant la multi-nazionale Accenture. Dal 2013 ha iniziato a lavorare full-time nel settore Bitcoin, cryptocurrencies e blockchain, partecipando alla fondazione e allo sviluppo di numerose start-up in un contesto internazionale (Italia, Svizzera, Canada, Malta, Panama). Nel 2015 ha creato a Milano un polo di Ricerca e Sviluppo su queste tecnologie, che è cresciuto fino a diventare uno dei principali hub del settore a livello globale (proprio a Milano sono nati alcuni standard di fatto dell'industria, come "Bolt" per il routing di Lightning Network e "Opentimestamps" per gli usi notarili della blockchain), generando l'iniziativa internazionale BHB Network, di cui è Direttore, e la rete di realtà industriali che a questa si affiancano (Svizzera, Canada, UK, Bulgaria, Ucraina, Sudafrica, ecc.).

WORKSHOP

LA DATA BREACH NOTIFICATION: OBBLIGHI E PROCEDURE

Tra gli obblighi che sono stati introdotti dal Regolamento europeo sulla protezione dei dati rientra quello di avere una procedura per la gestione delle violazioni di dati personali. Queste violazioni, note con l'espressione data breach, sono definite come "violazioni di sicurezza", a rimarcare ancora una volta la centralità della sicurezza e della gestione del rischio nel GDPR. Al fine di non farsi cogliere impreparati, progettare un piano di analisi e risposta ai data breach è diventata un'esigenza di tutte le aziende, le quali hanno 72 ore per comunicare all'Autorità di controllo l'avvenuta violazione. Questo lasso di tempo, tuttavia, rischia di essere del tutto insufficiente se non si è proceduto ad effettuare prima alcune valutazioni sulla natura dei dati presenti in azienda e a predisporre degli strumenti di contenimento del danno.

Pierluigi Perri, **Università degli Studi di Milano**
insegna Informatica giuridica avanzata ed è il coordinatore del Corso post laurea in Data protection e data governance. È stato Program Officer presso il Cybercrime Committee del Council of Europe a Strasburgo, Visiting Researcher nel dipartimento Corporate and Legal Affairs di Microsoft Inc. a Redmond, Visiting Postdoctoral Associate presso l'Information Society Project della Yale Law School e Non-Residential Fellow del Center for Internet and Society della Stanford University.
Autore di due monografie e di numerosi contributi scientifici in materia di diritto dell'informatica e information security, è inoltre condirettore della Collana "Informatica giuridica" edita da Giuffrè e vice direttore della rivista "Ciberspazio e diritto". È componente del Consiglio scientifico di AIPSI (Associazione Italiana Professionisti

Sicurezza Informatica) e membro dello Scientific & Technical Committee dell'Italian Chapter di IISFA (Information Systems Forensics Association).

DA NOBODY A 'ROOT'. COSA VUOL DIRE FARE ATTIVITÀ DI SICUREZZA OFFENSIVA

I membri di un red team sono spesso visti come qualcuno in grado di compiere magie con un browser ed un prompt. Un semplice host si tramuta in una porta attraverso la quale, durante un penetration test, si può entrare per prendere il controllo di un network più complesso.
Anche se spesso legato ad attività criminali, la compromissione di un sistema è anche parte essenziale del processo di validazione di un setup di un server o del deploy di un'applicazione web destinata al cliente finale.
Durante il talk percorreremo i vari passaggi che si incontrano durante un'attività di offensive security osservandone l'applicazione su server preparati ad hoc per essere violati da chi vuole approfondire

l'apprendimento della sicurezza offensiva, o da chi vuole semplicemente divertirsi un po', risolvendo qualche challenge senza avere problemi con la legge.

Il punto di partenza sarà quello di un attaccante attestato ad una rete che non conosce.
Da qui, vedremo a fine del talk di quanti sistemi riuscirà ad essere amministratore.

Paolo Perego *è uno specialista di sicurezza applicativa, 41enne che e vive a Milano.*
Quando non buca siti o insegna a scrivere codice sicuro, sviluppa numerosi strumenti di security che tiene sul suo spazio su GitHub (https://github.com/thesp0nge).
Mantiene un blog in italiano sulla sicurezza applicativa, https://codiceinsicuro.it e su twitter lo trovi seguendo @thesp0nge.
E' un marito e padre orgoglioso di Daniele e Anna ed è anche cintura nera 2 DAN di Taekwon-do ITF.

IL LATO OPERATION SECURITY DELLA CYBER RESILIENCE

Il punto più debole di ogni architettura di Security è sempre il fattore umano: l'operatore finale.
Per questo il giusto completamento di una struttura di CyberSecurity non può prescindere da alcuni aspetti di Operation Security che fungono da integrazione di ogni firewall aziendale.
Nella narrazione parleremo di:

- La Clean Desk Policy con i suoi sotto insiemi:
  - La classificazione (non IT) della documentazione cartacea (Pubblica, Confidenziale e Riservata)
  - Le regole sulla chiusura degli uffici durante la giornata e a fine giornata (con valutazioni anti-incendio)
  - L'archiviazione della documentazione (Confidenziale e Riservata) a fine giornata
  - Le famigerate password sui post-it
- La funzione del SecurPrinting
- I controlli da parte del personale di Security durante la notte
- L'importanza di una Operational Cyber Security Induction (via webinar per esempio) per i nuovi assunti e per il personale in generale sui temi di cui sopra

Matteo Tassoni, Country Security & Crisis Manager, (Italy, Balkans, Greece & Israel) - ABB SpA
Uscito dalla facoltà di Giurisprudenza a Bologna consegue un Master in Security Management a Roma ed inizia ad occuparsi di Security già dal 1999.
Con background quindi di tipo manageriale e non militare si occupa nel tempo, con ruoli crescenti, prima della funzione Security in Bartolini - Corriere Espresso a Bologna per poi spostarsi a Milano in Sicurglobal (ora Axitea) dove cura la parte operativa delle centrali satellitari del Gruppo.
Si sposta poi a Budapest dove lavora per il Gruppo MOL (Oil&Gas) dove cura la security sia per l'upstream (Pakistan, Kurdistan e Oman) che per il downstream (raffineria di Mantova).
Passa poi ad Avis Budget Group dove cura prima l'Italia e l'acquisizione di Maggiore Rent per poi prendere la responsabilità anche di Francia e Benelux.
Da maggio 2017 è il Security Manager di ABB Italia SpA per la quale cura la sub-region Italia, Grecia, Balcani ed Israele oltre ad avere la responsabilità Europea del Center of Expertise relativo al Project Security.

SICUREZZA E INTERNET OF THINGS

La crescente diffusione di sistemi di Internet of Things sia in ambito consumer sia in ambito di industria 4.0 rappresenta una grande opportunità ma nasconde delle inevitabili minacce. I produttori e gli utilizzatori di tali dispositivi, infatti, non sempre aderiscono a best practice di sicurezza dei device, le quali vengono ormai espressamente richieste dalla legge. La mancata progettazione sicura o l'implementazione non corretta di un sistema IoT può, quindi, comportare diverse responsabilità con un'esposizione ai danni molto elevata sia in termini di tutela dei dati personali posseduti dall'azienda sia in termini di tutela del patrimonio aziendale e della proprietà industriale. In questo workshop si esamineranno i requisiti giuridici di sicurezza dell'IoT e si traccerà una possibile roadmap sulla loro corretta adozione.

Pierluigi Perri, Università degli Studi di Milano
insegna Informatica giuridica avanzata ed è il coordinatore del Corso post laurea in Data protection e data governance. È stato Program Officer presso il Cybercrime Committee del Council of Europe a Strasburgo, Visiting Researcher nel dipartimento Corporate and Legal Affairs di Microsoft Inc. a Redmond, Visiting Postdoctoral Associate presso l'Information Society Project della Yale Law School e Non-Residential Fellow del Center for Internet and Society della Stanford University.
Autore di due monografie e di numerosi contributi scientifici in materia di diritto dell'informatica e information security, è inoltre condirettore della Collana "Informatica giuridica" edita da Giuffrè e vice direttore della rivista "Ciberspazio e diritto". È componente del Consiglio scientifico di AIPSI (Associazione Italiana Professionisti Sicurezza Informatica) e membro dello Scientific & Technical Committee dell'Italian Chapter di IISFA (Information Systems Forensics Association).

LA NUOVA ERA DELLE INVESTIGAZIONI DIGITALI: PASSATO, PRESENTE E FUTURO

La Digital Forensics è a un punto di svolta. Fino ad ora, poteva quasi esser definita una scienza "statica": quando avvengono degli incidenti i PC, server, traffico di rete e posta vengono analizzati per andare alla ricerca delle prove lasciate dall'attaccante. Ma oggi il futuro sembra indicare una nuova prospettiva di analisi ... con l'avvento della Cyber Threat Intelligence, ho provato, per la prima volta, una metodologia totalmente innovativa: la Digital Forensics insieme alla Cyber Threat Intelligence.

Lo scopo di questa presentazione è di spiegare in che modo questa nuova metodologia investigativa può essere applicata ad ogni tipo di incidente informatico come minacce interne, spionaggio industriale etc.., soprattutto, al beneficio che ne possono trarre tutte le tipologie di aziende e organizzazioni.

Selene Giupponi
Segretario Generale IISFA (International Information System Forensics Association) e Membro Fondatore di ECSO (European Cyber Security Organization). E' Cyber Security Advisor e Senior Digital Forensics expert per numerosi uffici della Procura della Repubblica, NATO, ITU (ONU). Fa parte dell'Advisory Board of Courage Cybercrime e CyberTerrorism European Research Agenda, membro del Comitato Scientifico dello schema di Certificazione ICT UNI11506:2013 AICQ-SICEV. Membro della Commissione ICT dell'Ordine degli Ingegneri della Provincia di Latina. Laureata in Ingegneria Informatica con Master in Computer Forensic e Digital Investigations. Docente in numerosi master Italiani e Internazionali in ambito Cyber Security, Cyber Defence e Digital Forensics.

TESTIMONIANZE

CYBER RESILIENCE: UN'OPPORTUNITÀ PER LE AZIENDE VIRTUOSE

Le Aziende che si confrontano quotidianamente con le sfide del mercato devo organizzarsi in maniera consapevole per gestire i rischi cyber. I servizi essenziali erogati dalle Società che gestiscono infrastrutture critiche devono essere garantiti in continuità, attraverso una attenta politica preventiva, una reattiva gestione degli incidenti ed una efficace interazione con le Autorità istituzionali.

Alessandro Manfredini, Responsabile Group Security A2A
Chief Security Officer del Gruppo A2A. Ha conseguito le Lauree in Giurisprudenza all'Università "La Sapienza" di Roma e in Scienze della Sicurezza interna e esterna presso l'Università di Tor Vergata di Roma.
Dopo un decennio di esperienza come Ufficiale dei Carabinieri è stato Security Manager del Gruppo Espresso e Direttore della Sicurezza Aziendale e dei Servizi Generali di Nuovo Trasporto Viaggiatori.

Tutor in conferenze, seminari, corsi di formazione anche a livello universitario si è specializzata in Enterprise Security, in protezione dei dati, fraud management e modelli di organizzazione e gestione.
È Segretario Generale di ACFE (Association of Certified Fraud Examiners) e membro del Consiglio Direttivo di AIPSA (Associazione Italiana Professionisti della Security Aziendale).

INFORMATION SECURITY AWARENESS: UNA PRIORITA' ASSOLUTA PER IL BUSINESS

La sensibilizzazione sulla sicurezza delle informazioni è una priorità imprescindibile per l'azienda moderna di qualsiasi settore e dimensione che voglia favorire l'allineamento della sicurezza con gli obiettivi e le strategie aziendali e proteggere al meglio il proprio business. Nel panorama moderno, la tecnologia digitale è onnipresente nei processi aziendali, le minacce informatiche si evolvono e i rischi di impatti sul business si moltiplicano. Quando la tecnologia fallisce, l'ultimo baluardo è la persona, che però, come insegnano recenti casi di cronaca, spesso è anche l'anello debole della catena. Scopriamo quindi come strutturare un programma aziendale di educazione e sensibilizzazione sulla sicurezza – con l'esempio di una campagna premiata dal Clusit – e quali sono i benefici in termini di cultura aziendale, di riduzione dei rischi e di supporto e protezione del business.

Ettore Guarnaccia, Professionista dell'ICT e dell'information security
Certificato CGEIT, CISSP, C|CISO, MoR e LA EN ISO 27001, esperto di normative e vigilanza bancaria in ambito IT, opera da oltre 20 anni nel settore ricoprendo incarichi di responsabilità in importanti realtà bancarie italiane e internazionali. Responsabile del settore Digital Identity & Access Management di Intesa Sanpaolo, in precedenza è stato CISO e responsabile del governo del sistema informativo e delle esternalizzazioni IT del Gruppo Popolare di Vicenza. Da diversi anni è educatore e formatore sulla sicurezza dei minori in istituti scolastici e sensibilizzatore in eventi pubblici indirizzati agli adulti. Nel 2016 ha lanciato il progetto "Generazione Z" per la rilevazione dell'esperienza dei minori e dei relativi fattori di rischio nell'uso delle moderne tecnologie digitali che diventerà presto un libro

THE HACK GAME

THE HACK GAME: DON'T TRY THIS AT HOME!

The Hack Game è un "gioco" dedicato alla formazione in ambito Cyber Security.
Dopo un breve momento iniziale di formazione tecnica Ethical Hacker, per rendere tutti i partecipanti autonomi nella scoperta di vulnerabilità e problematiche di sicurezza dovute ad errata configurazione e/o mancati aggiornamenti, il gioco si svolgerà in piccoli gruppi.
Ogni gruppo avrà a disposizione 3 Access Point con 3 misure di scurezza differenti che le squadre o i singoli dovranno "craccare" in modo da ottenere accesso alla rete "bersagli", per ogni rete Wi-Fi saranno presenti 2 server vulnerabili. Ogni partecipante avrà a disposizione un computer preparato con tool e sistemi dedicati all'attacco offensivo (sì avete capito bene, offensivo, simuliamo infatti il comportamento di un Cyber Criminale per capire il rischio che corriamo ogni giorno).
Lo scopo del gioco è quello di sensibilizzare gli attaccanti in ambito Cyber Security, così che imparino a conoscere le tecnologie ed evitare eventuali problemi di sicurezza.
E questo è solo l'inizio, tante sorprese durante il "gioco" ed un'ultima sfida nascosta che metterà a dura prova la passione e il know-how di chi colpirà il bersaglio.
Durante la formazione ed il "gioco" non verranno trascurati gli aspetti seri della sicurezza informatica e dei dai personali.

Condotto da Pawel "okno" Zorzan Urban, Cyber Security Manager, Hacker, Penetration Tester - Undisclosed
Nasce nel 1984 in Polonia, da sempre una passione per il cercare di capire come funzionano le cose per poterle controllare, proprio questa passione lo ha portato all'utilizzo delle tecnologie informatiche ed elettroniche per lavoro e passatempo personale.
Nei primi anni 90 inizia il suo percorso da Hacker nelle reti IRC internazionali entrando in contatto con hacker e "smanettoni" di tutto il mondo.
E' relatore presso i principali eventi Cyber Security, Scuole e Università Italiane.
Esperto in sicurezza di Networking e Wifi, da più di 17 anni si occupa di Penetration Test e Vulnerability Assessment, ha collaborato con diverse organizzazioni militari, governative e private segnalando gravi vulnerabilità ed aiutando i relativi Team ICT a risolvere tali problematiche.
Oggi è consulente strategico per diverse organizzazioni pubbliche e private.
Certificazioni e Metodologie utilizzate: CCNA1, CCNP, CEH, ACSE, OSSTMM, OWASP.

EXHIBITOR INSIGHTS

EVOLUZIONE DELLE MINACCE E APPROCCIO INTEGRATO ALLA CYBER DEFENCE

Gli attacchi informatici sono una realtà: in uno scenario in cui non è possibile bloccare tutte le minacce, il modo in cui un'azienda risponde agli attacchi è fondamentale.
Oggi la sicurezza informatica e la gestione del rischio cyber sono una delle priorità del business e come tali devono essere valorizzate, facendone comprendere l'importanza a tutti i livelli dell'azienda.
La complessità crescente degli attacchi rende necessaria una strategia e metodologia che realizzi una difesa proattiva e globale, che permetta di intercettare e gestire efficacemente segnali al fine di bloccare con tempestività l'attacco; è altresì necessario uno scambio di informazioni a livello non solo nazionale ma internazionale. Una sicurezza multilivello che integri Threat Intelligence, AI e machine learning per aiutare le aziende a scoprire i più sofisticati attacchi in qualsiasi fase del loro sviluppo.

Marco Zanovello, Program Manager Yarix - Cyber Division Var Group
Marco Zanovello è Program Manager presso Yarix, Cyber Division di Var Group. Laureato in Ingegneria elettronica all'Università degli Studi di Padova nel 1995, ha frequentato diversi corsi di formazione specialistica e ottenuto numerose certificazioni in materia di sicurezza informatica, Penetration Testing ed Ethical Hacking. E' Lead Auditor ISO 27001 dal 2009. Svolge consulenza per progetti nazionali ed internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling. Svolge inoltre attività di ricerca e sviluppo tramite collaborazioni con enti di ricerca in Italia e all'estero. Ha partecipato come relatore e docente a numerosi seminari e corsi presso enti pubblici e privati, associazioni, convegni.

CYBERSECURITY & "ENTERPRISE OF THINGS": LA SICUREZZA IN AZIENDA QUANDO TUTTO È ORMAI CONNESSO

Con l'emergere di Internet of Things/Enterprise of Things e dei loro miliardi di dispositivi connessi anche in azienda, il panorama dei rischi è cambiato in modo aggressivo: ciò a cui un intruso può accedere o modificare ora include veicoli, dispositivi medici e macchinari industriali solo per iniziare. I vantaggi per la società nel collegare tutti questi endpoint stanno diventando sempre più chiari, così come i rischi reali che si presentano lasciando anche un solo ed unico endpoint vulnerabile.
La sicurezza delle imprese è a volte paragonata alla costruzione di un castello per difendersi da un'orda infinita. Il successo non è tanto nel superare gli invasori, quanto nel contrastarli efficacemente in modo tale che si dirigano altrove alla ricerca di un attacco più facile: investire di più in difesa di quanto un aggressore sia disposto a spendere per l'attacco.
Ma è arrivato il momento di pensare in modo diverso e iniziare a prendere in considerazione attacchi invisibili e sconosciuti provenienti da questi miliardi di endpoint interconnessi. La scala delle minacce e delle potenziali aree di attacco è a un livello completamente nuovo e si espande quotidianamente.

L'impresa moderna non è più un castello ma un regno interconnesso che richiede una maggiore sicurezza per gestire minacce mai individuate prima.
La buona notizia è che BlackBerry ha affrontato a lungo questi problemi, ascoltando i propri clienti e sviluppando software, servizi e procedure che si sono evoluti per navigare meglio in questo regno e mitigare i rischi di attacco.

Diego Ghidini, Sales Director, BlackBerry Italia
La sua responsabilità comprende vendite e strategia commerciale su un mercato che va dalle PMI fino alle grandi aziende, dove BlackBerry è un punto di riferimento per le soluzioni EMM - Enterprise Mobility Management e per la sicurezza.
Prima di approdare in BlackBerry Ghidini ha avuto esperienze significative sia in Italia che all'estero dove ha ricoperto ruoli importanti e di crescente responsabilità nell'ambito delle vendite e del marketing. Fra gli incarichi precedenti più recenti, Ghidini è stato Direttore Vendite di Tiscali dove ha lavorato sia in Italia che in Europa e prima ancora è stato Country Manager per Madge Networks, dove oltre all'Italia ha seguito i paesi del bacino mediterraneo e quelli arabi del golfo persico.
Con oltre 20 anni di esperienza alle spalle, Ghidini ha passato buona parte della sua carriera nell'ambito dell'information technology e delle telecomunicazioni, fino a ricoprire l'attuale posizione.
Classe 1968, Ghidini è sposato ha 3 figli ed ama praticare sport.

DATA VALUE OR DATA KILLER?

I dati e le informazioni hanno un valore sempre più strategico all'interno delle organizzazioni, ne sono diventate un asset fondamentale.
La loro valorizzazione, gestione e tutela è quindi parte, o dovrebbe esserlo, della strategia aziendale.
Molte organizzazioni stanno rafforzando la propria capacità di gestione del cyber risk passando da una conduzione che sinora è stata prevalentemente delegata ai reparti tecnici, ad una di tipo risk management, attraverso la definizione di strategie di governo, modelli di valutazione e conseguentemente con interventi di mitigazione del rischio. Si tratta in molti casi di primi passi verso una gestione più strategica del cyber risk che però richiede un approccio molto diverso da quanto fatto sinora.
Uno degli elementi di cambiamento è la ponderazione dei diversi metodi di mitigazione del cyber risk, che tipicamente portano alla valutazione, possibile solo a seguito di una preventiva analisi e misurazione economica dello stesso, di quanto di questo rischio debba essere mitigato con interventi interni ad esempio organizzativi o tecnologici, quanto ceduto a terzi ad esempio tramite outsourcing di attività o assicurazione, e quanto ci si possa consentire di mantenere.
Una non corretta gestione di questa strategia può avere conseguenze catastrofiche, trasformando l'informazione dà valore a killer di un'organizzazione.
Cosa fare quindi? Come va approcciato il tema? Con quali modelli o strategie?

Pamela Pace, Partner Obiectivo

Azienda specializzata in business security che propone un'offerta di servizi di Cyber Security Strategy, Information Security Governance, Risk Intelligence, Risk Management.
Negli anni ha rivestito molteplici incarichi di crescente responsabilità nel campo dell'innovazione e delle tecnologie. Ad oggi è Componente della Commissione Tecnologie, Sicurezza e Mobile Payment dell'Associazione Italiana Istituti di Pagamento e Moneta Elettronica; Vicepresidente della Piccola Industria di Unindustria e componente del Comitato Tecnico Nazionale Ricerca ed Innovazione di Confindustria.
È inoltre membro del comitato direttivo del Centro Ricerche Nuove Tecnologie e Processi di Pagamento dell'Università degli Studi Internazionali di Roma e docente in ambito cyber security presso la Scuola di Palo Alto.