NEWSLETTER
30 maggio 2017

Clusit
Associazione Italiana per la Sicurezza Informatica

INDICE

Speciale Security Summit Roma 2017

1. Presentazione

Sono aperte le iscrizioni al Security Summit di Roma (https://www.securitysummit.it/event/Roma-2017) che si terrà nei giorni 7 e 8 giugno presso l'Auditorium della Tecnica - Viale Tupini, 65. (https://www.securitysummit.it/location/Roma-2017)

Il programma completo è disponibile anche su https://www.securitysummit.it/event/Roma-2017/agenda

La partecipazione al Security Summit e a tutti gli eventi che lo compongono è libera e gratuita, con il solo obbligo di iscriversi online su https://www.securitysummit.it/event/Roma-2017/register

2. Programma del 7 giugno

08:45 **Registrazione**

09:15-11:00 **Auditorium - Sessione plenaria**

PRESENTAZIONE DEL RAPPORTO CLUSIT 2017

Il Security Summit si aprirà con la presentazione del Rapporto Clusit 2017, frutto del lavoro di più di un centinaio di esperti e della collaborazione di un gran numero di soggetti pubblici e privati, che hanno condiviso con Clusit informazioni e dati di prima mano e condiviso le proprie esperienze sul campo.

Moderano: Corrado Giustozzi e Alessio Pennasilico, Clusit

Intervengono:

- Nunzia Ciardi, Direttore del Servizio Polizia Postale e delle Comunicazioni
- Andrea Zapparoli Manzoni, Clusit

Partecipano alla tavola rotonda:

- Angelo Bosis, Oracle
- Gastone Nencini, Trend Micro
- Federico Santi, DXC Technology

Tutti i presenti in sala potranno ritirare una copia del rapporto (fino ad esaurimento).

11:00-11:30 **Coffee break e visita all'area espositiva**

11:30-13:00 **Sala A – Percorso Professionale sulla Gestione della Sicurezza**

I DATI PERSONALI ALL'OMBRA DELLA NUVOLA: ESSERE CONFORMI AL GDPR NONOSTANTE IL CLOUD O GRAZIE AL CLOUD?

La corsa all'adeguamento al GDPR è ufficialmente aperta. Oggi praticamente ogni azienda ha già adottato qualche soluzione in Cloud, o progetta di farlo, pertanto il percorso verso la conformità deve passare necessariamente anche per la nuvola.
Comprendere quali siano gli impatti del Regolamento nel il contesto aziendale è un'attività di per se complessa; identificare gli adempimenti, e attuarli, in uno scenario Cloud (anche ibrido) introduce una serie di tematiche su cui è opportuno fare chiarezza: dati da proteggere altrove, processi interni supportati da applicazioni SaaS, esigenze di governance… Tuttavia, sorprendentemente, vi sono anche delle opportunità in questo scenario che rischiamo di non cogliere: scopriamole assieme!
Relatori: Luca Bechelli e Feliciano Intini

11:30-13:00 **Sala G - Percorso Professionale Tecnico**

SICUREZZA A 360° - WELCOME TO THE FUTURE OF CYBERSECURITY

Relatori Andrea Zapparoli Manzoni e David Gubiani

11:30-12:15 **Sala 6 – Atelier Tecnologico**

ANDIAMO IN CLOUD CON SICUREZZA

L'adozione di soluzioni in Cloud favorisce l'accesso e l'utilizzo di servizi e applicazioni da qualsiasi luogo e attraverso una pluralità di dispositivi, ma la necessità di garantire un alto livello di sicurezza dei dati e delle modalità di accesso ai servizi, rappresenta oggi la priorità per chiunque intenda intraprendere il percorso di innovazione verso il Cloud. La sicurezza e integrità dei dati, le normative e il controllo delle identità e degli accessi sono tra i principali aspetti da considerare affinché le soluzioni adottate possano garantire e soddisfare un utilizzo in sicurezza delle piattaforme e dei servizi in Cloud.
Vantea, Smart e Oracle propongono un approfondimento su questa nuova era dell'IT, illustrando i punti di attenzione da considerare e come questi possano essere gestiti mediante l'utilizzo di soluzioni Oracle che garantiscono un corretto processo di autenticazione/autorizzazione ai servizi, un controllo dell'accesso ai dati memorizzati sul Cloud e una governance complessiva e sicura delle infrastrutture Cloud e ibride.
Relatori: Ettore Fabbiano e Angelo Bosis

12:15-13:00 **Sala 6 – Atelier Tecnologico**

CONNECTED THREAT DEFENSE: L'UNICO APPROCCIO POSSIBILE ALLA SICUREZZA

Relatore: Alfredo Di Gennaro

13:00-14:00 **Lunch-Buffet e visita all'area espositiva**

14:00-15:30 **Sala A – Percorso Professionale Tecnico**

GESTIONE DEL RISCHIO E NUOVI SCENARI DI ATTACCO: COME RIDURRE IL RISCHIO APPLICANDO IL CONCETTO DI "LAYERED DEFENCE"

L'evoluzione delle minacce più moderne richiede lo sviluppo di un approccio integrato di difesa che si basi su una strategia multi livello.
Il Layering è uno dei concetti fondamentali nella sicurezza delle informazioni e diventa ancora più importante nel complicatissimo scenario di attacco attuale.
Il numero complessivo di malware prodotti al secondo ha raggiunto una cifra impressionante, altrettanto quanto il valore relativo mercato illegale che lo sostiene, in costante aumento. Il 2016 ad esempio è stato l'anno peggiore per il Cybercrime in Italia (Rapporto CLUSIT 2017) ed il Paese è stato vittima degli hacker, risultando per la prima volta nella top ten globale per numero di vittime strette nella morsa del ransomware.

Per contrastare efficacemente questo panorama è necessario considerare un vero cambiamento nelle strategie di difesa adottando nuovi aspetti tecnologici, un nuovo paradigma e soprattutto un approccio di Risk Management, anche in funzione del nuovo panorama normativo che sempre di più aiuterà le aziende a maturare sotto il profilo della sicurezza delle informazioni. L'evoluzione delle tecniche di attacco informatico e la dinamicità dei threats rendono inoltre sempre più complessa la valutazione quantitativa del rischio aziendale, spesso conducendo all'adozione di misure di prevenzione inadeguate o falsandone i relativi piani e budget. Partendo da una visione Enterprise Risk-based delle problematiche di information security e seguendo i riferimenti NIST e ISO 27005, porremo soluzioni di protezione end-point e di memory-introspection e casi aziendali a confronto per identificare il ruolo della tecnologia nell'abbattimento del rischio. Considerati sia gli aspetti tecnici, che il differente contesto di manifestazione dei threats, sarà quindi possibile giungere ad una più affidabile valutazione quantitativa.
Relatori: Andrea Zapparoli Manzoni, Denis Cassinerio, Gianluca Gravino e Leonardo Zanus.

14:00-14:45 **Sala G – Atelier Tecnologico**

LA CYBER SECURITY DEL SISTEMA BANCARIO HA FATTO UN BEL SALTO

La minaccia cyber, con le sue caratteristiche di pervasività e mutevolezza, ha fatto sì che il sistema bancario italiano, come in altre rilevanti occasioni, sia riuscito a cogliere un'opportunità di cooperazione e condivisione mirata a elevare la cyber defence dell'intero settore.
Relatori: Sabina Di Giuliomaria e Armando Leotta

14:00-14:45 **Sala 6 – Atelier Tecnologico**

LE EVOLUZIONI DEL SECURITY TESTING: DALL'ASSESSMENT AL CONTINUOUS MONITORING

Relatori: Guido Milana e Matteo Galimberti

14:45-15:30 **Sala G – Atelier Tecnologico**

LA MORTE ANNUNCIATA DELL'AV TRADIZIONALE, DEL SANDBOX E SIGNATURE BASED PREVENTION FRAMEWORKS

Nel 2017 le metodologie utilizzate dal CyberCrime sono cambiate.
Si è passati da File based attacks a File-Less, memory based, shellscripti, powershell based attacks dove a volte non vengono più utilizzati gli exploits nei files. Questo rappresenta una grande minaccia per tutte le soluzioni tradizionali basate sullo studio matematico di files. Infatti, non esistendo un file da analizzare/detonare nell' attacco complessivo, risulta impossibile l' identificazione e di conseguenza anche la generazione di AV signature updates, NGFW signature updates, IPS signatures ecc. Stiamo entrando in una era dove il "Cyber Crime" comincia ad utilizzare Machine Learning negli attacchi informatici.
SentinelOne è stata fondata nel 2013 da un gruppo Israeliano di esperti in cyber security che hanno sviluppato un approccio radicalmente nuovo e rivoluzionario per la protezione degli endpoint.
Soluzioni statiche e signature-based si rivelano inadeguate contro le minacce informatiche e la mancanza di integrazione tra i differenti strumenti di risposta agli incidents, rende le aziende altamente vulnerabili a causa dell'ampio intervallo che intercorre fra la fase di rilevamento e la remediation.
SentinelOne combina prevenzione, rilevamento e risposta in un'unica piattaforma, guidata da sistemi sofisticati di machine-learning e di automazione intelligente. Con SentinelOne, le aziende saranno in grado di rilevare il comportamento dannoso su molteplici vettori e di eliminare le minacce in maniera rapida grazie alla capacità di risposta integrata e completamente automatizzata.
Relatore: Jose Muniz

14:45-15:30 **Sala 6 – Atelier Tecnologico**

DATACENTER SECURITY: SICUREZZA OLTRE IL CICLO DI VITA DELL'OS

Gestione e Protezione del lifecycle delle infrastrutture it di servizio: virtual patching, compliance, protezione del dato, audit trail degli amministratori di servizio.

Relatori: Alessandro Ghezzi e Sunil Venanzini

15:30-16:00 **Coffee break e visita all'area espositiva**

16:00-16:45 **Sala A – Atelier Tecnologico**

AGILE NEI SERVIZI DI CYBER SECURITY

Nello scenario attuale Agile è una delle carte vincenti per offrire ai propri Clienti servizi di Cyber Security che generano il loro valore in poco tempo. Durante lo speech, dopo una breve introduzione, sarà descritta - tramite esempi e casi reali - la metodologia utilizzata in un contesto internazionale per i progetti di Security Testing ed Ethical Hacking.

Relatori: Simone Onofri e Fabrizio Tocci

16:00-16:45 **Sala G – Atelier Tecnologico**

RESILIENZA AL RISCHIO + DUTTILITÀ ORGANIZZATIVA = SUCCESSO DURATURO

In un contesto in cui il rischio cyber è in constante aumento ed in cui i trend attesi sono di una crescita esponenziale non è possibile pensare che la sola risposta tecnica possa essere la soluzione. Il cyber risk è un problema economico, sociale, politico, personale, colpisce al cuore della società civile e non risparmia niente e nessuno.

Come ci si deve preparare quindi a rispondere a quella che sarà la minaccia del nostro secolo? Come potranno le nostre, aziende e le nostre economie sopravvivere ad una tale offensiva?

La risposta è articolata e si muove su tanti livelli diversi che organicamente si devono sviluppare ed applicare in primis nelle nostre aziende centro nevralgico della sussistenza della nostra società. Una strategia che si basi su analisi tecniche, adeguamento organizzativo, supporto all'evoluzione culturale dell'organizzazione tutta ed una capacità di prevedere ed attuare rapidi adeguamenti sono gli elementi fondamentali per un successo duraturo.

Di questo ed altro parleremo durante la nostra sessione di lavoro.

Relatori: Pamela Pace e Alessio Pennasilico

16:00-16:45 **Sala 6 – Atelier Tecnologico**

MISURE DI SICUREZZA E PROTEZIONE DEI DATI PERSONALI: GDPR E ISO27001 SI INCONTRANO

Il nuovo regolamento privacy europeo GDPR spinge l'acceleratore sulle misure di sicurezza, riconosciute a tutti gli affetti come uno dei Principi da osservare nel trattamento dati personali e che comportano maggiori responsabilità per Controller e Processor, anche in considerazione delle pesanti sanzioni amministrative previste in caso di inadempienza.

Ma come scegliere misure adeguate rispetto ai rischi che hanno impatti sui diritti e le libertà fondamentali degli individui?

In attesa delle future 'certificazioni privacy' previste dal GDPR, vediamo come lo standard ISO27001 fornisca sin da subito base concreta per un approccio efficace da seguire nella scelta delle misure commensurate ai rischi specifici in tema di trattamento dati personali, anche alla luce della recente guida fornita da ENISA.

Vedremo infine, coerentemente con l'approccio metodologico sopra delineato, come sia possibile abilitare specifici controlli di sicurezza attraverso tecnologie di virtualizzazione e nuove architetture che trovano applicazione nei data center moderni e in contesti di hybrid cloud.

Relatori: Gloria Marcoccio e Matteo Indennimeo

16:45-17:30 **Sala A – Atelier Tecnologico**

COME AFFRONTARE LE NUOVE MINACCE DELLA CYBERSECURITY IN ITALIA: RANSOMWARE E ATTACCHI MIRATI NELLA PROSPETTIVA KASPERSKY

Relatore: Fabio Sammartino

16:45-17:30 **Sala G – Atelier Tecnologico**

COME RAGGIUNGERE LA CONFORMITÀ PCI DSS SEMPLIFICANDOSI LA VITA

Nonostante lo standard PCI DSS (relativo alla gestione delle carte di pagamento e oggi giunto alla versione 3.2) abbia una vita più che decennale, la sua applicazione rimane ancora estremamente complessa ed articolata. Il risultato è che la decisione, per un'azienda, di dover affrontare il percorso per raggiungere la conformità (ormai sempre più richiesta) può sembrare una sfida ardua.
Tuttavia, sfruttando i giusti accorgimenti, è possibile diminuire SENSIBILIMENTE la complessità e la tortuosità del percorso riducendo il perimetro e conseguentemente i requisiti applicabili.
Durante l'intervento saranno esaminati due punti di vista differenti: quello dell'auditor che ha l'obiettivo di valutare e validare la conformità dei requisiti e quello di un service provider che effettua attività di riservazione alberghiera gestendo transazioni "Card Not-Present" tramite un canale e-commerce e che ha affrontato e completato con successo il percorso di conformità PCI DSS riducendo il perimetro di analisi mediante l'adozione di specifici accorgimenti.
Inoltre, dal punto di vista consulenziale, sarà illustrata una recente soluzione definita e validata dal PCI Council che permette una sensibile riduzione del perimetro PCI DSS applicabile a realtà aziendali quali, ad esempio, negozi che accettano pagamenti "Card Present".
Relatori: Giusva Fiumana, Massimiliano Monterumisi, Paolo Sferlazza

16:45-17:30 **Sala 6 – Atelier Tecnologico**

DA THREAT INTELLIGENCE A THREAT HUNTING… LA NATURALE EVOLUZIONE DELLA SPECIE

Cosa succede quando ci si rende conto che la Threat Intelligence non basta a risolvere il problema? Eppure eravamo tutti convinti di aver imboccato la giusta strada…
Adesso che la consapevolezza della consistenza e della pericolosità delle minacce cyber è stata raggiunta non solo dagli esperti di sicurezza, ma anche (finalmente) dai vertici delle organizzazioni, ci si sta rapidamente accorgendo che non ci può essere alcun meccanismo, per quanto avanzato, che possa sostituire l'intuito e la capacità di reazione dell'analista umano.
Il nuovo paradigma è la «Threat Hunting», la caccia alle minacce. Ma come si possono combinare in un giusto mix la Threat Intelligence, attuata con soluzioni automatizzate quali «advanced analytics» e tecniche di «machine learning», con l'analisi dei dati realizzata da «cacciatori» umani di IoC (Indicators of Compromise)? Probabilmente la ricetta sta nel considerare la Threat Intelligence l'inizio - e non la fine - del processo, come in una «naturale» evoluzione della specie in cui il fattore abilitante rimane sempre la valutazione dinamica del rischio.
Relatori: Gabriele Liverziani e Davide Bernardi

17:30-18:15 **Sala A – Atelier Tecnologico**

E-MAIL SECURITY: COME INTERCETTARE LE MINACCE DEL GIORNO ZERO

Oggi è maggiormente importante e rilevante intercettare le minacce ancora sconosciute, piuttosto che identificare quelle già note. Circa 30mila nuove varianti di ransomware ogni anno, decine di nuove campagne di phishing ogni giorno: il canale di diffusione principale è l'e-mail.
Alimentato e motivato da un giro d'affari di centinaia di milioni di euro, il business del malware evolve continuamente.
Nel corso dell'atelier si illustrerà la continua evoluzione delle tecniche di attacco via e-mail e come impostare una difesa altrettanto reattiva, capace di identificare una minaccia ignota che appare per la prima volta.
Relatore: Rodolfo Saccani

17:30-18:15 **Sala G – Atelier Tecnologico**

DATA SECURITY E CONFORMITÀ NORMATIVA NEL CLOUD

Mitigare i problemi di sicurezza e i requisiti di conformità, giungendo alla definizione di un "punto di controllo" che si frappone tra gli utenti e il Cloud Service Provider in modo da intervenire nell'applicazione delle politiche di sicurezza aziendale nel momento in cui si accede alle risorse in Cloud: questo servizio di protezione aggiuntivo è oggi noto con il nome di Cloud Access Security Broker (CASB) definito dagli analisti come futura best practice e con una previsione di adozione pari all'85% entro il 2020.
I CASB (Cloud Access Security Broker) consentono di potenziare la moltitudine di politiche di sicurezza associate all'uso dei servizi sulla nuvola, qualsiasi essi siano. Questi offrono, infatti, un ampio raggio di funzionalità tra cui offrire analisi di dettaglio agli amministratori dei sistemi rispetto ai servizi in Cloud. I CASB, infatti, svolgono varie attività: consentono di utilizzare modelli pacchettizzati, personalizzare le policy, integrare soluzioni di machine learning per monitorare i comportamenti e far emergere attività rischiose. Sono tool on-premise e/o cloud-based, che idealmente si collocano tra chi usa i servizi in cloud e chi li fornisce, combinando le diverse politiche di sicurezza aziendale rispetto alle risorse sulla nuvola rese accessibili in chiave on demand.
Sinergy e Symantec presentano un approccio tecnologico per "governare" il fenomeno Cloud in grande crescita nelle aziende. Verrà mostrato come sia possibile "osservare" tale fenomeno e ridurre il rischio dell'azienda, mappando le procedure e le normative con un approccio tecnologico. Sarà evidenziata l'importanza di "vedere" cosa viene spostato nel cloud e da chi, introducendo quindi eventuali contromisure di controllo.
Relatori: Maurizio Costa e Giuseppe Marullo

17:30-18:15 **Sala 6 – Atelier Tecnologico**

...FALLO CON J.4.R.V.I.S.

In un contesto in cui il numero medio di vulnerabilità è cresciuto quattro volte negli ultimi quindici anni, non è più sostenibile gestire la securizzazione dei sistemi con le indicazioni del "solito vuappitti" fatto periodicamente ad opera di fornitori diversi, non sempre efficaci. E' quindi necessario rilevare, valutare e gestire le vulnerabilità infrastrutturali e applicative secondo metodi semplici ma efficaci, come vogliono le best practice in materia di vulnerability management.
Mettendo a fattor comune standard, good practice e tante fonti aperte, e con un occhio di riguardo alla compliance e all'asset management, ecco J4rvis: la vulnerability management suite per portarvi oltre il "solito vuappitti".
Relatore: Francesco Morini

3 Programma dell'8 giugno

08:45 **Registrazione**

09:15-11:00 **Auditorium – Tavola Rotonda organizzata e gestita da UNINDUSTRIA - Piccola Industria**

LE PMI ALLA SFIDA DELL'INNOVAZIONE E DELLA CYBER SECURITY

In quella che ormai viene definita la 4a rivoluzione industriale, dove l'accesso alle informazioni di qualsiasi genere avviene praticamente in tempo reale e grazie alle quali, attraverso il fattore abilitante delle tecnologie sempre più spinte, ogni modello di business è drasticamente cambiato, tutte le aziende - ma soprattutto le PMI - si trovano nella necessità di ripensare se stesse. Avere aziende smart capaci di accompagnare i costanti e sempre più veloci cambiamenti attraverso il mutare di modelli organizzativi, di processo, umani e tecnologici sarà, unitamente al know how ed alla qualità dell'offerta, il fattore che determinerà sopravvivenza e crescita delle stesse.
Per realizzare questo, però, è necessario portare nelle nostre aziende una cultura che veda nel cambiamento e nell'innovazione un'opportunità e non soltanto un rischio.
Ed è proprio attraverso questa cultura che le nostre PMI, asse portante dell'economia italiana, potranno veramente cominciare a strutturarsi adeguatamente per il futuro.
In questa sessione affronteremo nello specifico il tema dell'innovazione anche tecnologica quale driver di sviluppo, ne analizzeremo inoltre gli impatti negativi la dove questa non venga correttamente integrata all' interno dei processi di gestione aziendale.
Parleremo quindi del tema del cyber risk, indissolubilmente correlato all'innovazione tecnologica, e dei possibili danni anche economici prodotti da un attacco.

9:15-11:00 **Sala A – Percorso Professionale sulla Gestione della Sicurezza**

VULNERABILITY MANAGEMENT: DA INCUBO A PROCESSO ECONOMICAMENTE SOSTENIBILE

Solo un processo di vulnerability management ben strutturato può aiutare a gestire la complessità delle moderne organizzazione. Molti incidenti dovuti ad attacchi, infatti, si realizzano a causa di problemi causati dalla mancanza di gestione di tale complessità, ancor prima che per gravi problemi tecnici o di competenza.
Per questa ragione diventa indispensabile inserire questo processo nel framework di governance della cyber security, formando le persone per essere preparate a gestirlo e dotandole degli strumenti necessari a poter essere efficaci ed efficienti. La corretta gestione delle vulnerabilità, infatti, rende l'impatto economico di tale processo/formazione/strumenti di molto inferiore rispetto all'impatto degli incidenti (certi) che si verificherebbero altrimenti.
Relatori: Alessio Pennasilico e Fabrizio Cassoni

9:15-10:15 **Sala G – Atelier Tecnologico**

L'ENTERPRISE IMMUNE SYSTEM: COME USARE IL MACHINE LEARNING PER LA 'NEXT-GENERATION' CYBER DEFENSE

In questo atelier si illustrerà:

- come il 'machine learning' e la matematica stanno automatizzando la rilevazione delle minacce avanzate, attraverso le labili linee di confine della rete
- perché la tecnologia self-learning, conosciuta come approccio "immune system", rileva le minacce, non appena cominciano a manifestarsi, senza l'uso di regole e firme
- come ottenere il 100% di visibilità della rete in ambienti fisici, IoT, virtuali e Cloud, compresi i servizi Cloud e SaaS forniti da terze parti
- esempi di minacce "nel mondo reale" scoperte da Darktrace.

Relatore: Corrado Broli

10:15-11:00 **Sala G – Atelier Tecnologico**

MITIGAZIONE DI ATTACCHI DDOS SU LARGA SCALA - I VANTAGGI DI COMBINARE SICUREZZA E PRESTAZIONI NEL CLOUD

Durante il workshop condivideremo l'esperienza maturata dagli ingegneri di Cloudflare, nell'ambito della sicurezza e accelerazione di siti e applicazioni web, proveniente dalla gestione di piu' di 6 milioni di siti.
In particolare illustreremo nel dettaglio alcuni dei più grandi attacchi rilevati a livello mondiale, dal 2013 al 2016, e come si possono mitigare mettendo a confronto tecniche di mitigazione e limitazioni di una infrastruttura locale verso un'infrastruttura cloud distribuita.
Relatori: Michael Tremante e Maurizio Monti

11:00-11:30 **Coffee break e visita all'area espositiva**

11:30-13:00 **Auditorium – Percorso Professionale Legale**

SICURAMENTE GDPR

Come si deve affrontare il progetto di adeguamento della misure di sicurezza richieste dal nuovo Regolamento Europeo 679/2016 sulla Data Protection?
Quali sono? Da dove partire? Che relazione hanno le attività correlate con le iniziative già presenti in azienda? Che punti ci sono in comune con la Direttiva 680/2016 sullo stesso tema ai fini di prevenzione del crimine?
Questa sessione si articola in due fasi:

- Panoramica degli articoli di legge più rilevanti per l'IT, spiegazione di uno schema di riferimento
- Discussione tra gli esperti e domande dal pubblico

Introduce e modera: Alessandro Vallega, Direttivo Clusit, Europrivacy.info, Oracle
Con la parecipazione di:

- Bruno Bernardi, CSQA Certificazioni
- Luca Boselli, KPMG Advisory
- Vittorio Gallinella, LazioCrea
- Nicola Sotira, Poste Italiane

11:30-13:00 **Sala A – Percorso Professionale Tecnico**

UNDERSTANDING THE CYBER-ATTACKS: THE CYBER-KILL CHAIN

I mutevoli scenari dei cyber-attacchi, la loro frequenza, sofisticazione e target, richiedono una più efficace combinazione di prevenzione, rilevamento e risposta.
Molte organizzazioni necessitano oggi di tecnologie di protezione in grado di rilevare e bloccare gli attacchi di nuova generazione.
Nonostante gli investimenti fatti dalle aziende, #WannaCry ha dimostrato la necessità di adottare un nuovo modello di sicurezza.
Relatori: Alessio Pennasilico e Gianluca Busco Arre'

11:30-13:00 **Sala G – Percorso Professionale sulla Gestione della Sicurezza**

ADVANCING CYBER RESILIENCE: LA CYBERSECURITY PARLA IL LINGUAGGIO DEL BUSINESS

Il tema della Cybersecurity ha raggiunto rapidamente nel corso degli ultimi anni una visibilità assoluta ed ha assunto un ruolo prioritario per il Board ed il Top Management delle aziende di tutto il mondo. Le risposte tecnogiche sono essenziali, ma a dare delle risposte concrete deve essere il management delle aziende, a cui devono essere fornite informazioni comprensibili, integrate ed integrabili con la visione di business e con la gestione dei rischi di impresa.
Serve dare risposta a domande molto puntuali come: quanto sono esposto ai rischi? Quali interventi sono necessari? Quanto è necessario spendere?

Nella sessione presenteremo i diversi punti emersi da uno studio elaborato dal World Economic Forum, Boston Consulting Group e Hewlett Packard Enterprise. Il risultato derivante da questa collaborazione consiste in un framework e in una serie di strumenti, capaci di aiutare l'alta direzione delle aziende ad integrare il rischio e la resilienza Cyber nelle strategie aziendali.
Relatori : Hila Meller, Luca Bechelli, Davide Licciardello e Fabio Vernacotola

13:00-14:00 **Lunch-Buffet e visita all'area espositiva**

14:00-14:45 **Sala A – Atelier Tecnologico**

DIGITAL TRANSFORMATION: COME RIPENSARE LA SICUREZZA
La maggior parte delle grandi aziende hanno posizionato il tema della trasformazione digitale come un asse strategico della propria visione. Nonostante l'apparente conflitto tra 'operations' e 'IT' la sicurezza e la compliance sono elementi che consentono di valorizzare le attività di entrambi.
Relatore: Francesco Armando

14:00-14:45 **Sala G – Atelier Tecnologico**

"DETECTING THE UNDETECTABLE": IDENTIFICARE E RISPONDERE AI CYBER ATTACKS ANCHE QUANDO IL TUO AVVERSARIO NON USA MALWARE
Relatore: Stefano lamonato

14:00-14:45 **Sala 6 – Percorso Professionale Legale**

IL VOTO ELETTRONICO: POTENZIALITÀ E RISCHI LUNGO LA STRADA DELLA DEMOCRAZIA ELETTRONICA.
Mentre imperversano le post-verità sul voto americano, circa la verosimile ingerenza cibernetica dei russi sull'elezione di Trump e siamo a solo qualche mese di distanza dal referendum costituzionale italiano, è impossibile non interrogarsi su quanto il voto elettronico, prassi consolidata oltreoceano, seppur malamente, potrebbe interessare, almeno in termini di semplificazione, le procedure nostrane.
Una valutazione sulla sua attuabilità andrebbe infatti operata, se non altro, a fronte delle immani difficoltà nel riuscire a garantire il diritto di voto in situazioni, ad esempio, di emergenza.
Stati Uniti e Italia occupano inoltre, a ben vedere, due posizioni estreme in materia di e-voting politico: da un lato vi è un paese che è stato pioniere nell'adozione del voto elettronico, dall'altro uno in cui si usano carta e matita. In mezzo, paesi che lo stanno valutando e altri che, come l'Olanda, l'hanno adottato e poi abbandonato per motivi di sicurezza.
Relatori: Federica Bertoni e Claudio Telmon

14:45-15:30 **Sala A – Atelier Tecnologico**

ARTIFICIAL INTELLIGENCE VS MALWARE. LA NUOVA GENERAZIONE DELLA SICUREZZA DIFENSIVA
Nello scenario di attacchi sempre più complessi in cui si combinano Rootkit e Zero-Day exploit, ad avanzate tecniche di evasione è necessario mutare radicalmente il paradigma di difesa. Le soluzioni tradizionali dimostrano i propri limiti nella capacità di analisi, protezione, risposta e tecniche di anti-detection; vogliamo analizzare lo scenario delle tecnologie attuali e quelle emergenti, fornendo una visione pratica di come indirizzare questa evoluzione.
Durante l'atelier si organizzerà anche una dimostrazione in tempo reale di come queste nuove tecnologie possano essere efficacemente adottate per rilevare e mitigare attacchi ransomware oltre che per attivare triage and response su attacchi complessi come quelli portati con tool di sistema e completamente in memory.
Relatore: Marco Zonta

14:45-15:30 **Sala G – Atelier Tecnologico**

BOOLEBOX: LA STRATEGIA VINCENTE PER TENERE AL SICURO LE INFORMAZIONI DAI RANSOMWARE E MINACCE CHE VIOLANO LA PRIVACY DEI DATI RENDENDOLI INACCESSIBILI

L'attacco ransomware WannaCry, che lo scorso mese ha colpito almeno 150 Paesi e oltre 200mila client in tutto il mondo sfruttando alcune vulnerabilità di Windows, ha portato alla ribalta una questione complessa e quanto mai urgente, che attiene non soltanto alla gestione e alla protezione dei dati di privati e aziende, ma che riguarda l'intero sistema-Paese.
Relatore: Alfonso Lamberti

14:45-15:30 **Sala 6 – Percorso Professionale Legale**

MISURE MINIME DI SICUREZZA PER LE PUBBLICHE AMMINISTRAZIONI: UNA NUOVA NORMATIVA, SEMPLICE DA COMPRENDERE ED EFFICACE NELLA SUA IMPLEMENTAZIONE

Relatore: Corrado Giustozzi

15:30-16:00 **Visita all'area espositiva**

16:00-16:45 **Sala A – Seminario a cura di UNINFO**

NUOVI TREND E NORME ISO/UNI: BLOCKCHAIN, IOT, BIG DATA, INDUSTRY 4.0 E CERTIFICAZIONI "PRIVACY"

Con l'evolversi delle tecnologie e dei framework organizzativi la normazione sta diventando sempre più un tavolo di confronto evolutivo, dove confluiscono nuove idee e vengono consolidati i trend vincenti del mercato.
UNINFO, l'ente di normazione nazionale federato a UNI per l'ICT, vi propone delle anteprime a coinvolgendo i propri esperti di spicco sui temi più "caldi" oggi in discussione che daranno forma negli anni a venire ad un mercato che comprende organizzazione di tutti i tipi: dall'erogazione di servizi alla produzione alla consulenza.
Relatori: Domenico Squillace, Fabio Guasconi e Luciano Quartarone

16:00-16:45 **Sala G – Tavola Rotonda**

INCONTRO CON I CERT ITALIANI

Modera: Corrado Giustozzi
Intervengono:

- il CERT Nazionale
- il CERT PA
- il GARR-CERT
- il CERT di Poste Italiane

16:00-16:45 **Sala 6 – Seminario a cura di ASSINTEL**

VIGILARE, DISSEMINARE, MAI DISSIMULARE… RISCHI, PROSPETTIVE E PROTEZIONE DEL BUSINESS DELLE MPMI

16:45-17:30 **Sala A – Seminario a cura dell'Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale (ANORC)**

LE NOVITÀ DELL'AUDIT DI CONFORMITÀ NELLA PUBBLICA AMMINISTRAZIONE. NUOVE REGOLE, NUOVI RUOLI E PROFESSIONALITÀ DELL'AUDITOR

Il Regolamento europeo 910/2014 ha introdotto un nuovo modello di controllo per i cosiddetti servizi fiduciari.
Il Legislatore italiano si è adeguato al di là degli obblighi regolamentari comunitari e ha esteso il modello di conformità tipico delle certificazione ISO 9001 e 27001 anche ai servizi soggetti ad accreditamento e vigilanza pubblica come SPID, la PEC e la Conservatoria digitale.

Nel seminario si descrivono le nuove regole per l'attestazione della conformità, il ruolo di AgID e di ACCREDIA. Si parlerà anche dei nuovi ruoli e professionalità degli auditor in evoluzione e conformità alla ISO/IEC 17025:2005.
Relatore: Giovanni Manca

16:45-17:30 **Sala G – Seminario a cura del CIS - Università La Sapienza di Roma**

I CONTROLLI ESSENZIALI DI CYBERSECURITY E LA LORO RELAZIONE CON IL FRAMEWORK NAZIONALE
La sessione presenterà i 15 Controlli Essenziali di Cybersecurity definiti dal Centro di Ricerca di Cyber Intelligence e Information Security della Sapienza (CIS-Sapienza) e dal Laboratorio Nazionale di Cybersecurity e la loro relazione con il Framework Nazionale per la Cybersecurity.
I controlli possono essere adottati ed implementati da medie, piccole o micro imprese per ridurre il numero di vulnerabilità presenti nei loro sistemi e per aumentare la consapevolezza del personale interno, in modo da resistere agli attacchi più comuni.
I Controlli essenziali di Cybersecurity sono di facile e, quasi sempre, economica implementazione e rappresentano una serie di pratiche di sicurezza che, al giorno d'oggi, non possono essere ignorate.
Relatore: Luca Montanari

16:45-17:30 **Sala 6 – Seminario a cura dell'(ISC)2 Italy Chapter**

SICUREZZA DEL WEB 2.0: ANALISI DEL RISCHIO E CMS
Il Web 2.0 ha reso fruibile Internet a tanti ma, al contempo, ha aperto nuove importanti frontiere al rischio cibernetico.
La storia dell'informatica è piena di esempi di eccessive semplificazioni ergonomiche che hanno causato vulnerabilità facilmente sfruttabili (es. RPC, NetBIOS, WEP, etc).
Il Web 2.0 non fa eccezione a questa regola.
Può essere, però, adottato un approccio di Analisi del Rischio, esaminando gli obiettivi e le minacce peculiari del proprio Web 2.0 per determinare le priorità delle debolezze strutturali.
Queste, assieme alle caratteristiche della organizzazione, costituiscono una sorta di "impronta di vulnerabilità, in base alla quale determinare la migliore soluzione CMS da impiegare.
Relatore: Paolo Ottolino

17:30-18:15 **Sala A – Seminario a cura dell'Italian Chapter di IISFA (International Information Systems Forensics Association)**

TECNICHE DI SOCIAL NETWORK ANALYSIS APPLICATE ALLE INVESTIGAZIONI DIGITALI
Relatori: Marco Stella e Davide D'agostino

17:30-18:15 **Sala G – Seminario a cura dell'ACFE Central Italy Chapter**

"WHITE COLLAR CRIME E CRIMINAL PROFILING ATTRAVERSO L'ANALISI DELLE FRODI AZIENDALI"- ACFE REPORT TO THE NATION
Relatore: Michele Magri

17:30-18:15 **Sala 6 – Seminario a cura del Progetto "Romantic scam" (http://www.romantic-scam.eu/)**

ROMANTIC SCAM E SEXTORTION: TRUFFE AL CUORE DAL WEB. PRECAUZIONI E ISTRUZIONI PER NON DIVENTARE VITTIME
Una corretta informazione sui metodi di adescamento dei truffatori ed un uso consapevole del web rappresentano gli strumenti adeguati della prevenzione in rete affinchè ogni persona possa tutelarsi da ogni forma di imbroglio.
Informare, sensibilizzare i cittadini su queste truffa sentimentali, dare la corretta guida per riconoscerle e non diventarne vittima è lo scopo di Romantic Scam.
Relatrice: Letizia Mollo

4. Programma serale - Auditorium

7 GIUGNO - HACKING FILM FESTIVAL

La IX edizione dell'Hacking Film Festival, evento culturale "satellite" del Security Summit, è dedicata a cortometraggi e filmati indipendenti sul tema dell'hacking e della (in)sicurezza con la seguente programmazione:

7 giugno, orario 18.30 – 20.30
"ALLA SCOPERTA DELLA CITTÀ PIÙ PERICOLOSA DI INTERNET"
Diretto da Sean Dunne

Nel corso della sessione, Alessio Pennasilico e Luca Bechelli coordineranno un breve dibattito sui contenuti e ascolteranno e commenteranno le osservazioni del pubblico.

L'Hacking Film Festival è realizzato in collaborazione con la Facoltà di Informatica Giuridica dell'Università degli Studi di Milano. Si ringrazia il prof. Giovanni Ziccardi, responsabile scientifico del Festival.

Al termine, gli spettatori sono invitati a partecipare ad un rinfresco/aperitivo.

8 GIUGNO - EVENTO AIRA

Già in occasione del Security Summit di Milano, in marzo, Clusit aveva deciso di sostenere l'Associazione Italiana Ricerca Autismo (AIRA), conferendole un premio (un'opera d'arte realizzata dall'artista Roberto Pedrotti) per testimoniare dell'eccellenza dell'attività svolta nel campo della ricerca, aderendo alla 10a Giornata Mondiale della Consapevolezza sull'Autismo indetta dall'ONU nel mese di aprile.
In occasione del Security summit di Roma abbiamo desiderato continuare in questa opera di sostegno alla ricerca e di sensibilizzazione nel Paese, organizzando assieme ad AIRA un evento dal titolo "Disturbi dello spettro autistico: vissuti e sfide dei protagonisti".
L'evento, che farà da chiusura del Summit romano, si terrà nell'Auditorium dalle 18:30 alle 20:30 e vedrà l'intervento di numerosi ricercatori e professionisti impegnati da anni sul tema dell'autismo.

Moderano: Maria Luisa Scattoni e Paolo Giudice

Sono previsti i seguenti interventi:

Giovanni Valeri: "I disturbi dello spettro autistico: esperienza italiana e giordana"

Luigi Mazzone: "Comportamenti a problema e come affrontarli"

Daniele Lombardo - Giovanni Pioggia: "La tecnologia 'al servizio' delle persone nello spettro"

Stefania Stellino: "Cosa significa essere genitori di persone nello spettro?"

Raffaella Faggioli e Luca Vignando: "Dalla diagnosi all'autodeterminazione: cosa significa la diagnosi di disturbo dello spettro dell'autismo nella collaborazione fra clinici e pazienti"

Al termine, è previsto un rinfresco/aperitivo a cui siete tutti invitati.

LA PARTECIPAZIONE ALL'EVENTO È LIBERA E GRATUITA, MA È NECESSARIO ANNUNCIARE LA PROPRIA PRESENZA SCRIVENDO A info@clusit.it

5. Attestati e crediti CPE

Tutte le sessioni, tenute da esperti del mondo accademico e da professionisti del settore, danno diritto a crediti/ore CPE (Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP, CISA, CISM o analoghe richiedenti la formazione continua.

L'Attestato di Partecipazione viene rilasciato solo a chi ha assistito all'intera sessione e risulta regolarmente registrato.
Gli attestati saranno inviati, per email, solo a chi ne farà richiesta a attestati@clusit.it.

La registrazione è possibile solo online sul portale e non sono accettate altre modalità di registrazione come email o fax.

Le registrazioni potranno essere accettate anche direttamente alla Reception del Security Summit, ma non potrà essere garantita la disponibilità del posto in sala, né l'eventuale materiale didattico.

6. Gli sponsor del Security Summit Roma 2017

Sponsor Partner:
DXC Technology, MICROSOFT, TREND MICRO, ORACLE COMMUNITY FOR SECURITY (ORACLE e ORACLE ACADEMY partecipano assieme a quattro partner della community: ALFAGROUP, CSQA, KPMG, VANTEA SMART)

Sponsor Platinum:
BITDEFENDER, CHECK POINT, F-SECURE, PANDA

Sponsor Gold:
ADITINET, AIZOON, BOOLE SERVER, CLOUDFLARE, CROWDSTRIKE, CYTRIX, DARKTRACE, KASPERSKY, LIBRAESVA, QUALYS, SENTINELONE, SINERGY, SYMANTEC, VMWARE

Sponsor Silver:
BLACKSWAN, I DIALOGHI, SANS, SORINT.SEC

Sponsor Tecnici:
@MEDIASERVICE.NET, OBIECTIVO

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*
Dipartimento di Informatica - Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - cell. 347.2319285
* associazione senza fini di lucro, costituita il 4 luglio 2000