Programma CYBER CRIME CONFERENCE - 12 Aprile 2016 - Roma

Date : 5 aprile 2016

Le nuove minacce del Cyber Spazio

7a Edizione - 12 Aprile 2016 - ROMA
Centro Congressi Roma Aurelia Antica Via degli Aldobrandeschi, 223 - Roma

08:30 Registrazione Partecipanti

AULA 1 - Sessione mattina
“La rete come arma: la convergenza tra terrorismo e cyber-spazio”

Abstract: Attualmente lo Stato Islamico rappresenta senza ombra di dubbio la principale minaccia terroristica per tutti i Paesi occidentali. Il numero sempre più elevato di cittadini europei coinvolti in azioni terroristiche ha portato da tempo gli esperti del settore a riflettere in modo più attento e approfondito sui metodi e i mezzi utilizzati da questa organizzazione terroristica per radicalizzare e plasmare la mente dei futuri martiri. Ciò soprattutto in considerazione della loro distanza dai territori di radicalizzazione delle dottrine religiose e la loro vicinanza per nascita e per cultura ai principi occidentali.
In quest’ambito, uno degli strumenti maggiormente utilizzati ed efficaci, è senza dubbio la rete Internet.
La tavola rotonda intende approfondire queste tematiche mettendo a fuoco il ruolo che internet e le tecnologie hanno nella strategia dello Stato Islamico al fine di qualificare al meglio questa minaccia e delineare possibili soluzioni di contenimento.

9:30 - Tavola Rotonda
Modera: **Barbara Carfagna**, giornalista di TV7 e Speciale TG1

- On. **Andrea Manciulli**, Presidente della Delegazione italiana presso l’assemblea parlamentare della NATO
- **Stefano Mele**, of Counsel di Carnelutti Studio Legale Associato, Avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza delle informazioni e Intelligence

- **Claudio Neri**, Responsabile dell'Osservatorio sugli affari strategici ed internazionali dell'Istituto Italiano di Studi Strategici "Niccolò Machiavelli"
- On. **Domenico Rossi**, Sottosegretario di Stato del Ministero della Difesa (fatti salvi impegni istituzionali ad oggi non noti)
- Paolo Scotto di Castelbianco, Responsabile della comunicazione istituzionale e Direttore della Scuola del DIS

11:05
Gianni Baroni, Amministratore Delegato Gruppo Daman
Titolo: **Privileged Access Management - Come mettere al riparo le organizzazioni dal principale vettore di attacchi Cyber**
Abstract: La maggior parte delle violazioni alle misure di sicurezza informatica predisposte dalle organizzazioni private e pubbliche sono collegate agli “accessi privilegiati”, cioè a quei permessi che vengono concessi a personale interno o esterno all’organizzazione per le inevitabili attività di manutenzione ai sistemi e alle reti. Gli account che consentono di effettuare queste attività sono la strada maestra utilizzata del Cyber Crime, per violare la sicurezza perimetrale e inserirsi all’interno di una rete protetta senza lasciare alcuna traccia di questo accesso. La gestione efficace dei privilegi di accesso diventa quindi indispensabile per coniugare le esigenze di produttività con la necessità di proteggere gli asset critici, garantendo un accesso sicuro e controllato ai sistemi e alle reti.

11:30
Corrado Broli, Country Manager Italy Darktrace
Titolo: **L’Enterprise Immune System: il Machine Learning per rilevare le minacce sconosciute**
Abstract: Nel corso della presentazione si illustrerà:

- Perché le tecnologie "immune system" rappresentano una innovazione fondamentale per la cyber defence
- Come utilizzare il “machine learning” e la matematica per rilevare le minacce interne evolute
- Come ottenere il 100% di visibilità della rete per investigare le anomalie emergenti in tempo reale
- L’Enterprise Immune System e “Case Studies” reali

11:55
Michele Fiorilli, Pre-Sales Area Manager DGS e Joseph La Mela, Sales Manager Centro Sud Cyberark
Titolo: **I nuovi scenari per la protezione delle infrastrutture critiche**
Abstract: CyberArk, leader nella sicurezza degli account con privilegi, in partecipazione con DGS forniranno una panoramica a 360° sulla problematica della cybersecurity per le infrastrutture critiche. Si partirà dall’approccio da VA, Network Segmentation, Behaviour analisys, PIM e di come sia importante governare tutte queste fasi. La protezione dal perimetro verso l’interno e l’importanza di proteggere le organizzazioni dall’interno. Una percentuale compresa tra l’80 e il 100% di tutti gli incidenti gravi inerenti la sicurezza informatica riguarda la compromissione e l’utilizzo in modo illecito degli account privilegiati in una qualche fase

dell’attacco. Gli account privilegiati non gestiti adeguatamente rappresentano quindi una delle più serie minacce alla sicurezza per un’organizzazione, per questo motivo, bisogna estendere la protezione al di là di un singolo punto e garantire la sicurezza sia dall’esterno verso l’interno, sia viceversa. CyberArk è l’unica società che fornisce protezione completa contro le minacce avanzate sia interne che esterne per mitigare i rischi e rispondere ai più elevati requisiti di conformità.

12:20

Marcello Romeo, Presales Manager Italy, Intel Security

Titolo: **La Strategia di difesa contro le minacce sconosciute**

Abstract: Il volume e la complessità delle minacce sono in continuo aumento, mentre il tempo e le risorse per affrontarle sono in diminuzione, per cui i professionisti della sicurezza devono far evolvere la propria metodologia. Lo scopo dell'attività di difesa non è cambiato: proteggere i servizi e le informazioni vitali da furti, manipolazioni e perdite, dovuti ad attori interni ed esterni. Ciò che deve cambiare è il modo di lavorare, concentrandosi sulle modalità per ridurre la frammentazione della protezione, automatizzare le attività e moltiplicare le sinergie tra le misure di difesa vantaggio di un ecosistema di protezione adattativo.

Intel Security ritiene che un sistema aperto e integrato sia quello che meglio consente alle organizzazioni di bloccare efficacemente le minacce, identificare le compromissioni e velocizzare il processo di rimedio. Un mondo sicuro e connesso è al centro del nostro impegno. Grazie alle nostre soluzioni leader di protezione degli endpoint, alla differenziazione delle tecnologie e alla popolare piattaforma di gestione aperta e centralizzata, velocizziamo l'intero ciclo di vita delle difese: il Threat Defense Lifecycle.

12:45

Giuseppe di Somma, Presidente Cifit - Criminology International Forensic Investigation Thechnologies

Titolo: **La sicurezza del trasferimento dei dati a terra da un drone**

Abstract: Entro i prossimi cinque anni si ritiene che ci saranno in circolazione circa 10mila Droni (APR) civili, un giro d’affari che a livello mondiale si stima possa arrivare nel 2020 a 11 miliardi di dollari contro i 6,6 miliardi di quest’anno *(dati del Teal Group). Un processo di sviluppo inarrestabile. Nel futuro prossimo i cieli saranno sempre sorvolati.

Le organizzazioni per la difesa dei diritti civili e i parlamentari sollevano tuttavia il tema del rischio che i velivoli APR si rivelino un mezzo d’intrusione e sorveglianza nella vita dei cittadini, ma soprattutto in un momento cosi attenzionato verso le minacce del terrorismo, l’uso dei APR è un coltello a doppio taglio, grande strumento di controllo e di tutela, ma anche una potenziale minaccia.

Ci sono molte società specializzate che hanno sviluppato tecnologie di contrasto meccanico ed elettronico per inibire il volo dei APR su determinate aree, ma il punto più importante e da focalizzare è la protezione dei dati di trasmissione tra l’ operatore a terra e il Drone in volo.

Argomenti trattati:

- Il Drone capace di recarsi dove occhio umano non può giungere, importanza del monitoraggio video.
- Le capacità di applicazione dei droni nel campo della sicurezza e del’antiterrorismo (VIDEO).

- La comunicazione radiocomando tra operatore e il Drone e la trasmissione dei dati.
- Le tecnologie di contrasto meccanico ed elettronico per inibire il volo dei Droni (VIDEO).
- Il progresso tecnologico, l'industria dei Droni. Un processo di sviluppo inarrestabile.
- Il Droni come si evolveranno, un occhio sul Futuro (VIDEO).

13:10
Arije Antinori Phd, CRI.ME LAB "Sapienza" Università di Roma, Dip. di Comunicazione e Ricerca Sociale CORIS
Titolo: **Scenari futuri: l'evoluzione tecnologico-criminale ed il mutamento del conflitto in ambito metropolitano**
Abstract: La crescente evoluzione tecnologica fondata sullo sviluppo infrastrutturale delle reti, dei servizi alla cittadinanza e delle risorse mobili, è in grado di trascendere i confini territoriali, delle città, degli Stati e di dar vita a nuove dimensioni e spazi (cyber-)sociali sempre più pervasivamente integrati in uno scenario futuro caratterizzato dall'emersione di nuove vulnerabilità, a livello individuale, collettivo e di sistema. In tal senso, la crescita degli assets (cyber-)criminali, la proiezione dei fenomeni criminali complessi nel cyber-space ed il rilevante aumento del fenomeno del cosiddetto Crime-as-a-Service, favorirà l'espansione del "mercato" (cyber-)criminale, dando vita a dinamiche distorsive, devianti e criminali di crowdfunding, con l'avvento di vere e proprie operazioni di "crime-sourcing" anche al fine di compiere complesse e coordinate azioni tattico-aggressive in ambito metropolitano, determinando una significativa evoluzione del conflitto e della minaccia, in particolare sul fronte rispettivamente, criminale organizzato, eversivo e terroristico.

13:35 - Lunch e visita Area Espositiva

AULA 1 - Sessione pomeriggio
"l'Hacking Back e misure attive di difesa"

14:30
Corrado Giustozzi, Membro del Permanent Stakeholders' Group di ENISA ed esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT-PA
Titolo: **ENISA trend escape 2015**
Abstract: Come oramai tradizione Enisa, l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, ha pubblicato ad inizio anno un rapporto sul panorama della minaccia Cyber rilevata nel mondo durante l'anno precedente. L'intervento presenterà e commenterà i risultati più rilevanti emersi dal rapporto ETL (Enisa Threat Landscape) 2015.

14:55
Stefano Mele, of Counsel di Carnelutti Studio Legale Associato, Avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza delle informazioni e Intelligence
Titolo: **Hacking Back come forma di reazione legittima di uno Stato ad un attacco informatico**
Abstract: Comprendere se e come sia possibile per un governo contrattaccare in maniera legittima ad un attacco informatico effettuato da uno Stato o da soggetti terzi sponsorizzati da uno Stato rappresenta ormai un'esigenza imprescindibile. Soprattutto oggi che le dottrine

strategiche di un numero sempre maggiore di attori internazionali prevedono - ormai anche in maniera chiara ed esplicita - la conduzioni di operazioni informatiche offensive per ottenere vantaggi politici, strategici, economici e militari. L'intervento mira ad approfondire il panorama legale e normativo legato a questa problematica, delineando le finestre di opportunità e i punti critici.

15:20
Giovanni Giovannelli, Senior Sales Engineer Sophos Italia
Titolo: **Ransomware!? Se lo conosci lo eviti**
Abstract: I ransomware sono in continua evoluzione, riconoscerli è la prima forma di difesa che possiamo innalzar

15:45
Alessio Pennasilico, Security Evangelist
Titolo: **Subire o difendersi da un attacco: ma quanto costa?**
Abstract: L'efficacia nel contrastare un attacco dipende molto dal cosa si è fatto in anticipo. Decidere se e quanto investire prima, durante e dopo l'attacco dipende ovviamente dalla comprensione dei diversi rischi e dalle risorse che di conseguenza sono state destinate alla loro gestione.

16:10
Stefano Zanero, Professore associato, Politecnico di Milano
Titolo: La sicurezza dei sistemi cyber-fisici: una tempesta perfetta

17:00 - Chiusura Lavori

AULA 2 - Sessione mattina
"La cooperazione pubblico-privato tra i SOC e le Istituzioni"

Abstract: La rivoluzione digitale che ha cambiato i paradigmi dell'economia e della società in Italia, in Europa e, in diversa misura in tutti i paesi del mondo, porta con sé, oltre a enormi benefici, una serie di nuovi rischi. Da qualche anno si parla di cyber minacce e attacchi hacker ma oggi sono stati raggiunti livelli di consapevolezza e competenza molto elevati, anche alla luce di incidenti di vasta portata. Uno dei capisaldi in questo ambito è la collaborazione tra tutti gli attori che devono o possono occuparsi di sicurezza, dalle istituzioni pubbliche ai centri preposti alla cyber security, dalle aziende agli enti universitari e di ricerca, fino alla società civile. Lo scambio di conoscenze, standard e buone pratiche tra stakeholder deve anche avvenire, nell'odierna economia globalizzata, non solo su scala nazionale e europea, ma a livello mondiale, perché Internet ci ha insegnato che il regno del digitale, nel bene e nel male, non ha confini.
Con i nostri interlocutori del mondo istituzionale, dell'impresa privata e dei Security Operation Centers (SOC), nella tavola rotonda che segue andremo ad approfondire proprio con quali procedure i SOC collaborano con le istituzioni e il ruolo che questi centri svolgono nel prevenire e combattere il cyber crimine; ci faremo raccontare case studies e best practices e proveremo a indagare quali sono - se ci sono - le difficoltà in questo compito cruciale di monitoraggio della

sicurezza informatica, approfondendo in particolare il nodo della privacy, molte volte considerata antitesi della security.

9.30 - Tavola Rotonda
Modera: **Patrizia Licata**, giornalista di Formiche.net

- **Gerardo Costabile**, Head of Security & Safety at FASTWEB
- **Stefano Bargellini**, Director of Safety, Security, Property and Facilities at Vodafone Italia
- **Roberto Di Legami**, Direttore del Servizio Polizia Postale e delle Comunicazioni
- **Rita Forsi**, Direttore Generale Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione Ministero dello Sviluppo Economico ISCOM
- **Gian Luigi Savioli**, responsabile Security Monitoring & Incident Handling per Telecom Italia

11:05
Andrea Zapparoli Manzoni, Head of Cyber Security, KPMG Advisory SpA
Titolo: La funzione del CSIRT (Computer Security Incident Response Team) nel supportare il processo di Cyber Risk Management
Abstract: Il processo di Cyber Risk Management va alimentato in tempo reale tramite adeguate fonti di intelligence, relative sia all'esterno che all'interno. Per quanto riguarda il secondo ambito l'apporto informativo del CSIRT, se ben strutturato, è di sempre maggiore importanza e va opportunamente valorizzato

11:30
Isabella Corradini, Presidente centro ricerche Themis Crime e Luisa Franchina, Presidente di AIIC
Titolo: **La cybersecurity per gli "esperti" e per i "non addetti ai lavori"**
Abstract: In questo intervento il tema della cybersecurity viene affrontato partendo dal racconto di esperienze condivise dalle relatrici in ambito aziendale e nel normale contesto quotidiano. Ingegneria sociale, OSINT, comunicazione, fattore umano: queste alcune parole chiave dell'intervento.

12:20
Marco Zanovello, Program Manager Var Group, Security Team Yarix
Titolo: **Security Operation Center: Un approccio probabilistico per lo sviluppo di un modello previsionale**
Abstract: Presentazione di un modello previsionale volto a rilevare i trend delle minacce cyber basandosi su un approccio stocastico e probabilistico, a partire dai dati raccolti dal Security Operation Center di Var Group e Yarix, organizzati per tipologia di mercato, con riguardo anche a infrastrutture di natura pubblica ad alto rischio.
Per rispondere alle sfide migliorando difesa e sicurezza, il metodo proposto fornisce gli strumenti per comprendere se il verificarsi di un evento funga da elemento segnalatore dell’inizio di una minaccia tecnicamente più evoluta.

12:45

Silvia Portesi, Network and Information Security - Research and Analysis Expert at ENISA
Titolo: **Rapporto di ENISA Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches**
Abstract: The 2015 ENISA report on “Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches” aims to present:

- The regulatory and non-regulatory approaches of EU Member States as well as EEA and EFTA countries to share information on cyber incidents;
- The different sector regulation challenges of managing cyber security issues; and
- Their key practices in addressing these challenges.

The report identifies three types of approaches to share information on cyber security incidents: 1) traditional regulation; 2) alternative forms of regulation, such as self- and co-regulation; 3) other approaches to enable information sharing, such as information and education schemes. Core findings are:

- “The prevalence of traditional regulation, alternative forms of regulation (such as self- and co-regulation) and other approaches to enable information sharing on cyber incidents, varies from country to country;
- There is a general prevalence of alternative types of regulatory initiatives (co- and self-regulation) in the field of information sharing on cyber incidents;
- Different regulatory and non-regulatory approaches bring different challenges with them (as discussed in the following pages of this report);
- Trust is a key element for the success of the information sharing on cyber incidents;
- National and governmental CSIRTs play an important role in the field”.

Report available at:https://www.enisa.europa.eu/activities/cert/support/information-sharing/cybersecurity-information-sharing

13:10
Paolo Dal Checco, consulente informatico forense
Titolo: **Attività d'intelligence e digital forensics in ambito di attacchi, intrusioni e reati informatici: esperienze di passaggio d'Informazione dal piano tecnico a quello della comunicazione tra enti e privati.**
Abstract: Esistono diverse tecnologie e metodologie volte a monitorare le minacce che circolano in rete e che spesso sfociano in veri e propri attacchi e reati informatici verso aziende, privati o Enti Pubblici. Il tracciamento degli indicatori di compromissione spesso viene eseguito dai SOC, ma talvolta anche semplici IT Manager o Consulenti Tecnici sono in grado di identificare attacchi tramite intelligence o digital forensics. Entrambi si ritrovano poi con il compito di comunicare con le Istituzioni per gestire al meglio quanto rilevato. Con una buona cooperazione - non sempre facile da gestire ma in netto miglioramento - si ottiene l'effetto win-win per il quale sia SOC con i privati/consulenti sia le Istituzioni ne traggono beneficio ma, soprattutto, chi poi ne trova il vero giovamento sono le realtà finali che vengono protette.

13:35 - Lunch e visita Area Espositiva

AULA 2 - Sessione pomeriggio
“Botnet Takedowns: l’evoluzione nel cloud”

Abstract: Il nefasto fenomeno delle Botnet è conosciuto da tempo così come sono, ormai, ampiamente conosciuti i suoi risvolti in ambito di sicurezza informatica, di criminalità organizzata nonché quelli, strettamente connessi, di natura economica (intesi come guadagni illeciti ma anche come danni subiti dalle vittime). Le Botnet sono infatti delle concrete minacce non solo per le aziende ma, di fatto, per chiunque utilizzi un computer collegato alla Rete; come noto queste vengono impiegate quotidianamente per portare attacchi di ogni tipo quali, ad esempio, lo spam, il trafugamento di dati o attacchi di DDos. Nell'ultimo anno e mezzo si sta, poi, assistendo ad una loro ulteriore evoluzione: l’impiego di servizi Iaas per creare delle VM da usare appunto come Botnet.
La Tavola rotonda ha, quindi, lo scopo di fare il punto della situazione affrontando l’argomento delle Botnet in Cloud sotto svariati punti di vista quali ad esempio la cooperazione tra forze di polizia e cloud provider, l’analisi forensics nel Cloud in funzione dell’identificazione di queste tipologie di Botnet e dei relativi attacchi, il mercato dei malware nel deep web, sino ad affrontare la tematica della prevenzione con uno sguardo alla proposta della c.d. Direttiva Nis (Network and Information Security).

14.30 - Tavola Rotonda
Modera: **Valerio Vertua**, Vice Presidente di CSA Italy e Presidente di Digital Forensics Alumni

- Stefano Zanero, Professore associato, Politecnico di Milano
- Giuseppe Vaciago, Avvocato esperto in diritto penale societario e delle nuove tecnologie
- Carlo Mauceli, National Technology Officer di Microsoft Italia

15:35
Valerio Pastore, President, Chief Technology Officer e Fondatore di Boole Server
Titolo: **Dati cifrati e sotto controllo anche in mobilità. La tecnologia Cloud non è mai stata così sicura.**
Abstract: I sondaggi indicano che gran parte delle aziende italiane si sta orientando verso il passaggio al cloud con più o meno consapevolezza delle conseguenze che ne deriveranno. Se da un lato le potenzialità di uno strumento così versatile sono molteplici, dall'altro espone l’azienda a notevoli rischi nell'ambito della protezione dei dati.
Il passaggio ai servizi in cloud infatti aiuta a ridurre i costi, aumentare l’efficienza e offrire maggiore agilità ma è anche motivo di preoccupazione. L’incertezza dei CIO riguarda soprattutto l’efficacia della protezione del marchio, della proprietà intellettuale e del rapporto con i clienti.
Di pari passo allo spostamento verso il cloud va anche l’aumento dell’utilizzo dei dispositivi mobili per l’accesso ai dati che si trovano in cloud aumentando ulteriormente l’incertezza sulla loro sicurezza.
La risposta a queste esigenze apparentemente divergenti è rendere il cloud sicuro con un servizio che offra massima protezione ed estrema semplicità d’uso anche in mobilità, INSIEME.

16:00
Francesco Armando, Technical Account Manager Qualys Italia
Titolo: **Dal cloud un aiuto per contrastare il malware. E un pizzico di compliance.**
Abstract: Come avere una visione continuamente aggiornata della postura di sicurezza di un’organizzazione quando i numeri crescono? In un mondo in cui gli attacchi non conoscono pausa e gli essere umani cadono puntualmente nelle trappole mirate, è possibile pensare meno al paziente 0 e concentrarsi sulla prevenzione? Qualys offre una piattaforma di sicurezza integrata che permette di avere una visione della propria postura di sicurezza così come appare agli attaccanti. Un vaccino?

17:00 - Chiusura Lavori

Per maggiori informazioni ed iscrizione all'evento www.tecnaeditrice.com