PRIMO OSSERVATORIO ANFOV SULLA SICUREZZA NELLE INFRASTRUTTURE DI RETE

Una Panoramica sullo status della sicurezza delle infrastrutture di Rete in Italia, con interventi da parte di aziende utilizzatrici e fornitrici di prodotti per la sicurezza e di Auditors per la Sicurezza

21 GENNAIO 2014

MILANO

Presso la Sala Corsi del nostro associato Telecom Italia

Piazza Einaudi n. 8 – MM 2 Gioia

Le minacce e gli attacchi alle Reti sono sempre più evoluti: la rapida adozione dei social media, la diffusione di applicazioni web e le "policy BYOD" richiedono un nuovo approccio intelligente alla sicurezza.

L'aspetto che, tra l'altro, talvolta sfugge alle aziende italiane sono gli obblighi di legge imposti a chiunque abbia dati in forma digitale da gestire. In particolare le prescrizioni riguardano i dati personali e sensibili .

Per aiutare a proteggersi proattivamente dalle minacce in continua evoluzione, incluse quelle poste dai social media e dai siti web maligni, alcune aziende propongono, ed altre già adottano, oggi, una classe di applicazioni per la sicurezza della rete, che fornisce una vista più granulare del livello di sicurezza dell'azienda e un'interfaccia di gestione semplificata.

L'ANFoV, che da più di 20 anni, si occupa in vario modo di "temi concreti" che interessano tutti gli attori nel settore ICT/TLC, vuole, con la fondazione di questo Osservatorio sulla Sicurezza delle Infrastrutture di rete, fornire ai propri associati, oltre a un panorama aggiornato dei rischi in relazione ad attacchi ed a normative non osservate, anche esempi di applicazioni adottate o fornite da alcune aziende che operano in Italia.

PROGRAMMA:

10.00 – 10.15 - ACHILLE DE TOMMASO

Presidente ANFoV – Introduzione all'Osservatorio

10.15 – 10.45 - DARIO CARNELLI

Auditor per la Sicurezza della Rete e dei Sistemi

La sicurezza come necessità e come opportunità.

La circolazione delle informazioni e dei dati è oggi indipendente dalla nostra consapevolezza. La non consapevolezza si estende poi alle architetture tecnologiche ed ai rischi; tale non consapevolezza porta allo sviluppo di modelli inadeguati di "service and problem management"

10.45 – 11.30 – RENATO CONTI

IBM – Security - Technical Sales and Solutions Leader

Protezione contro le frodi e sicurezza in ambito cloud e mobile

Negli ultimi anni è cambiato il profilo dei criminali informatici, sia in merito agli obiettivi oggetto degli attacchi, sia per la sofisticazione delle tecniche utilizzate. Questa evoluzione è stata fortemente favorita nell'ambito dei nuovi scenari informatici caratterizzati dall'adozione di soluzioni cloud, dall'utilizzo dei dispositivi mobili, dalla diffusione dei social network e dall'esplosione della quantità e della varietà dei dati in rete. In questa situazione di forte apertura nell'accesso alle risorse IT, le aziende devono mettere in campo soluzioni avanzate per: proteggersi contro le frodi informatiche; mettere in sicurezza il canale di accesso mobile; adottare in maniera sicura il paradigma "cloud". IBM ha consolidato negli anni un portafoglio di soluzioni di sicurezza integrate che permettono di proteggere sia gli scenari IT tradizionali, sia quelli emergenti, consentendo alle aziende di condurre il proprio business in modo sicuro.

11.30 – 12.15 -PAOLO DA ROS

CRYPTONET – Partner

Nel corso degli ultimi 6-8 anni si e' diffuso un senso di inaadeguatezza per cio' che concerne la sicurezza delle reti. Si e' diffusa a macchia d'olio una serie di minacce di nuova generazione contro cui i sistemi difensivi oggi adottati sono impotenti e ciechi sul piano della rilevazione. Abbiamo sistemi capaci di individuare, bloccare e rimediare a tutte le minacce azzurre e quadrate, e chi attacca usa strumenti tondi e gialli.

le applicazioni mobili sono spessissimo delle vere e proprie applicazioni client server, con thick clients installati sui dispositivi degli utenti. La distribuzione delle applicazioni avviene tramite

piattaforme poco controllate o completamente incontrollate, da cui un attaccante puo' scaricare l'applicazione, effettuarne la reverse engineering, modificare alcuni contenuti, per poi salvare la app modificata sullo stesso app store o su un un app store " parallelo" .

12.15 – 13.00 - ROSARIO PIAZZESE - Director

SILEDO GLOBAL

Social Network: il mobile come abilitatore e la security come inibitore. Rischi e Opportunità

La velocità di diffusione dei social network ha creato un circolo alimentante con l'altrettanto rapida diffusione delle device mobili e del BYOD. Il ciclo di vita dei social è più condizionato dalla facilità di accesso che da logiche di controllo del rischio e di integrazione in approcci enterprise di gestione. La stessa percezione delle esigenze di presenza e di sicurezza su questi vettori di comunicazione sembra essere completamente asimmetrica rispetto alle normali logiche di gestione delle informazioni, ormai mature e consolidate. La valutazione dei rischi, pur noti ed evidenti, sembra oscillare tra la completa sottovalutazione o l'assoluta inibizione. Ma è possibile adottare dei modelli di controllo che tutelino senza inibire, che abilitino le opportunità della presenza senza enfatizzare le vulnerabilità, che qualifichino il BYOD come un'opportunità concreta ma effettivamente gestibile?

Nel corso dell'intervento verranno presentati alcuni spunti di riflessione e alcuni indirizzi concreti che facilitino la valutazione e permettano l'applicazione di logiche di misurazione e controllo anche su contesti così fluidi".

13.00 – 13 45 DAVID GUBIANI – SE Manager Italy

CHECK POINT

Security Report

Il report offre un'analisi degli eventi di sicurezza di rete che nell'ultimo anno hanno coinvolto le organizzazioni di tutto il mondo. Presenta gli eventi di sicurezza indentificati presso queste organizzazioni, con esempi relativi agli incidenti resi noti, spiegazioni di come alcuni di questi attacchi sono stati condotti, e raccomandazioni su come proteggersi da questo tipo di minacce.

LUNCH : 13.45 – 15.00

(segue)

15.00 – 15.45 GENSÉRIC CANTOURNET – Security / Cross Processes and Projects

TELECOM ITALIA

La sicurezza delle reti per Telecom Italia

Le telecomunicazioni sono eminentemente strategiche: energia, trasporto, banche, ecc.; non esiste settore che non ne usufruisca. Le telecomunicazioni non servono solo allo scambio di dati ma costituiscono un metodo di scambio e un mezzo di conoscenza per intere comunità di persone desiderose di condividere una cultura comune; diffondono le conoscenze che emergono dal nuovo modo di pensare il mondo. Dalla rete fisica scaturiscono reti virtuali che moltiplicano le possibilità di interconnessione e quindi di interagire. In particolare, Internet ha fatto nascere nuovi strumenti di collaborazione digitale nei quali i rapporti intesi paritari (pear-to-pear) si sviluppano più velocemente che le organizzazioni gerarchiche. Colonna vertebrale dell'insieme delle infrastrutture, le reti di telecomunicazioni devono essere legittimamente tutelate da minacce polimorfe digitali e non. Questa necessità diventa a tal punto pressante che l'informazione è un'assoluta condizione di competitività, soprattutto nei mercati che vedono il progresso delle nuove tecnologie aumentare non più in modo incrementale ma esponenziale. Come procedere quindi per proteggere la rete? Con processi pubblico-privati trasversali e sistemi integrati di protezione nonché una Governance dei rischi che ne consenta un trattamento idoneo e economicamente sostenibile, bilanciando tecnologia e investimenti, pur mantenendo la rete il più possibile aperta a tutti."

15.45 – 16.30 LUCA COMODI - Responsabile Area Network & Security Management

LABORATORI GUGLIELMO MARCONI

NAC e BYOD: soluzioni open source in ambito enterprise

Le tecnologie dell'informazione e delle telecomunicazioni supportano oggi i principali processi organizzativi, gestionali e decisionali di aziende e Pubbliche Amministrazioni. Sino ad ora, notevoli risorse sono state indirizzate alla protezione dei principali asset IT delle organizzazioni da attacchi esterni ai loro confini di gestione. Tuttavia, le politiche di Bring Your Own Device (BYOD) minano alla base le assunzioni su cui vengono comunemente definiti i perimetri di sicurezza dei sistemi informativi. Le soluzioni di Network Access Control (NAC) combinate a strumenti di port security, possono contribuire molto alla definizione e implementazione di politiche di sicurezza in grado di proteggere adeguatamente gli asset critici delle organizzazioni anche a fronte di attacchi interni ai confini gestionali del loro sistema informativo. L'intervento presenterà le esperienze di Laboratori Guglielmo Marconi nella realizzazione, implementazione e governo di soluzioni di NAC avanzate realizzate con strumenti Open Source e discuterà un case study dell'architettura implementata in ambito sanitario.

16.30 – 17.15 GIORGIO PARPINELLI - Director

EVOLVE

La steganografia: arte antica, minaccia moderna

La steganografia è una tecnica che ha lo scopo di nascondere la comunicazione tra due interlocutori, mantenendo nascosta l'esistenza di dati a chi non conosce la chiave atta ad estrarli. Si tratta di un'arte antica, che risale al quarto secolo A.C. che sta avendo una accelerazione grazie alle tecnologie digitali, le quali si prestano particolarmente allo scopo.

L'intervento vuole illustrare e dimostrare la facilità con cui si può utilizzare questa tecnica ed il grande rischio che essa rappresenta per le infoamzioni aziendali e non solo.

17.30 – CONCLUSIONE E TERMINE DEI LAVORI