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

RELAZIONE

Il primo osservatorio ANFoV sulla sicurezza nelle infrastrutture di rete si è tenuto a Milano il 21 gennaio 2014.

Obiettivo dell'osservatorio è fornire 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.

Achille de Tommaso, Presidente ANFoV ha introdotto l'osservatorio, richiamando anche il ruolo di ANFoV nello scenario italiano delle TLC. Il presidente ha ricordato che la sicurezza delle reti è fondamentale per abilitare il business di qualsiasi azienda e che le aggressioni sono sempre più frequenti e sofisticate. Tutte le aziende, anche le piccole, sono attaccabili e la maggior parte non è realmente attrezzata.

Dario Carnelli, Auditor per la Sicurezza della Rete e dei Sistemi, ha centrato il suo intervento sul fatto che la sicurezza può essere vista non solo come necessità ma anche come opportunità.

Oggi la circolazione dell'informazione supporta tutti i processi aziendali ed è fattore di innovazione. Le reti di comunicazione abilitano un numero sempre maggiore di interazioni, sia individuali sia aziendali. La comunicazione è anche elemento possibile di sviluppo, numerosi sono gli esempi di organizzazioni virtuali, dematerializzate e asincrone, consentite dalla possibilità continua di comunicazione. In ambiente bancario, ad esempio, ci sarebbero enormi opportunità di rivedere la supply chain sfruttando le opportunità della comunicazione. Fare innovazione oggi è fattore premiante e la comunicazione è elemento cardine dell'innovazione.

Ma che cosa significa sicurezza? Inalterabilità nel trasporto, confidenzialità, disponibilità, accessibilità, prestazioni. L'Italia risente di forti disparità geografiche rispetto a questi parametri. C'è anche una difficoltà di dialogo tra utilizzatori e fornitori, che necessita di essere superata. E' necessario aumentare la consapevolezza, un'associazione come ANFoV rappresenta uno snodo per la creazione di modelli e buone pratiche, oltre a interagire efficacemente con il potere regolatorio.

Renato Conti, Security System Division di IBM.

L'intervento ha riguardato la protezione contro le frodi e la sicurezza in ambito mobile. IBM ha una task force, X-Force, di 800 persone, che monitora costantemente il tema della sicurezza e fornisce dei report pubblici che illustrano i trend di maggior rischio (disponibili a http://www-03.ibm.com/security/xforce). Secondo l'indagine di X-Force, si registrano modalità di attacco sempre più complesse che utilizzano il social engineering, studiando il comportamento degli utenti in rete, per colpire in modo mirato.

Il mobile è una enorme opportunità per cyber criminal, nel caso in cui i "device" non siano correttamente governati. A livello business, un elemento di rischio è anche la quantità di dati presenti nei database aziendali: un non appropiato content management è grosso rischio potenziale di perdita di informazioni.

Comporre il mosaico della sicurezza, in risposta a questi rischi, è un processo complesso che richiede un approccio innovativo.

Conti ha presentato un caso tipico di una frode telematica, rispetto alla quale è stata definita una architettura di prevenzione, basata su un software che è una libreria di applicazioni, utilizzabili come Apps. Il primo livello è un agent software che previene il malware e gli attacchi Phishing. Il secondo livello è una metodologia nuova che riesce ad identificare il malware all'interno dei device. Come terzo livello, si offre anche un servizio di verifica sull'utilizzo del device: se si verificano condizioni anomale nell'utilizzo, vengono richieste autorizzazioni supplementari.

Il mobile, in generale, si basa su strumenti variamente utilizzati con comportamenti molto differenziati, dove coesistono reti con livelli di sicurezza diversi; per questo affrontare questo fenomeno è possibile solo con un approccio complesso e integrato.

In base al framework di analisi, IBM ha identificato tre aree critiche. Lato device: tracciare e gestire i device e settare le configurazioni in modo sicuro; lato rete, gli strumenti devono essere adeguatamente autenticati e costantemente monitorati; lato Apps, le Apps vanno sviluppate in maniera sicura seguendo best practice di sviluppo precise, che devono essere testate. Queste aree devono essere coperte se si vogliono mantenere gli standard di sicurezza.

Paolo Da Ros Partner di Cryptonet

L'intervento di Cryptnonet ha riguardato, tra l'altro, "La protezione dei VIP dalle minacce informatiche".

L'intervento ha illustrato storie istruttive di attacchi informatici (Lockhead e impianti per l'arricchimento dell'uranio) e delle tecniche utilizzate che permettono a chi li realizza di mantenersi silente per tempi anche molto lunghi, controllando completamente i flussi di informazione e i dati scambiati, con bassi rischi e investimenti. In generale, l'informatica è il modo più semplice per

controllare e quindi potenzialmente ricattare persone, soprattutto VIP; ed effettuare atti di terrorismo in generale. “Spear phishing” e “whaling” sono tecniche utilizzate per target mirati, tendenzialmente di alto livello. Le App su dispositivi mobili sono di fatto prive di protezione per la propria integrità, il loro codice binario può essere facilmente sottoposto a reverse engineering, tramite strumenti facilmente reperibili anche in rete. Cryptonet lo ha verificato, scaricando applicazioni mobili reperibili pubblicamente, ha realizzato il reverse engineering delle applicazioni, ricostruendo i sorgenti: le chiavi sono facilmente sostituibili e questo consente potenzialmente di violare non solo l’applicazione, ma di mettere in pericolo l’integrità dell’intero device. Esistono attacchi contro cui non c’è difesa, ciò che si può fare è rendere più difficile il loro compito.

Rosario Piazzese, Siledo Global SA

Siledo è uno spin-off di recente costituzione, che lavora nell’ambito della sicurezza, con focus sulle applicazioni mobili per i sistemi di pagamento, commercio elettronico e relativa IT governance.

Mobile e social network hanno enormi implicazioni riguardo alla sicurezza. Con modelli di validazione e accesso facili e poco controllati -attraverso social network, ad esempio- si veicolano anche informazioni relative ai pagamenti. Inoltre, molte delle tecnologie mobili che si utilizzano hanno implicazioni di sicurezza, a causa della consumerisation delle tecnologie portatili, ad esempio nel settore del credito al consumo. Social network e mobile devices presentano enormi opportunità ma devono essere adeguatamente presidiati. I rischi riguardano il rischio di conformità rispetto alle normative, il rischio operativo relativo alla sicurezza, il rischio relazionale riguardo a immagine e reputazione. La governance di questi fenomeni comprende la sicurezza dei dispositivi, la sicurezza delle applicazioni e dei dati e deve essere completamente integrata con l’intero contesto aziendale. E’ necessario monitorare e rendere consapevole il management dei rischi connessi all’utilizzo dei device, il mobile deve diventare un fattore qualificante ma la scommessa è impegnativa anche perché è in atto uno spostamento dei livelli di responsabilità legati al loro utilizzo. Chi mantiene l’ownership del rischio? In realtà allungandosi la filiera di intermediazione ci sono molti attori in gioco, storicamente poco integrati che devono invece trovare un terreno di confronto comune. Il supporto alle aziende che affrontano questi problemi deve anche cambiare con un approccio che tenga conto della necessità di trovare un trade-off tra le diverse necessità.

David Gubiani – SE Manager Italy CHECK POINT

Nel suo intervento, Gubiani, ha presentato i risultati di un report che illustra l’analisi degli eventi di attacco alla sicurezza in rete avvenuti nel 2013. Sono stati analizzati oltre 900 clienti, monitorando le informazioni che transitano attraveso la rete. Il report evidenzia una sconcertante percentule del 63% di aziende infette da Bots, praticamente tutte ignare di esserlo.

L’attacco normalmente parte dallo sfruttamento di vulnerabilità che consentono di prendere possesso di un certo numero di macchine all’interno di un’organizzazione. Si parte dall’identificazione di persone-target che, contattate attraverso i social network, fanno sì che le proprie macchine vengano infettate. Gubiani ha illustrato, tra gli altri, l’esempio di un attacco al New York Times e ha evidenziato la facilità con cui questi attacchi possono essere realizzati.

Per combattere questo fenomento, servono strumenti innovativi. I metodi di infezione sono i consueti: link, allegati ma soprattutto web applications (Java, Flash, Adobe, ecc…)., P2P applications e file sharing. Le aziende non sono normalmente attrezzate, mancano quasi sempre addirittura le policies di

riferimento. Anche la consapevolezza della perdita dei dati –che pure riguarda il 54% delle aziende analizzate- è scarsa, secondo il report presentato, e soprattutto, può essere tardiva.

Gensèric Cantournet – Vice Direttore Della Sicurezza Di TELECOM ITALIA

Intervento su: Security / Cross Processes And Projects

Obiettivo della security di Telecom Italia è la tutela delle infrastrutture critiche di comunicazione, nelle quali sono in gioco anche interessi a livello nazionale e internazionale.

E' in atto una generale evoluzione delle minacce cibernetiche, volume e qualità degli attacchi sono in aumento. I malware puntano soprattutto alle infrastrutture, non solo in senso fisico (reti, ferrovie, aeroporti) ma mirano a colpire anche il mercato servito e il servizio reso attraverso l'infrastruttura stessa. Tutte le infrastrutture sono interdipendenti e potenzialmente soggette ad un effetto domino.

Le misure adottate da Telecom Italia sono: ridondanza delle infrastrutture, ove possibile, di tecnologie in senso fisico e logico; sale operative integrate, crisis management e business continuity. Un altro elemento chiave nell'approccio di Telecom è la collaborazione, attraverso un sistema integrato- tra pubblico e privato.

La missione di Telecom è estremamente complessa. Le attività delle funzioni di security sono organizzate intorno al processo. E' stato fatto un enorme lavoro di protezione delle infrastrutture critiche, partendo dalla classificazione di siti e asset.

Cantournet ha fatto una carrellata di problemi di security, esemplificativi dell'approccio da parte di Telecom Italia, dall'accesso con i badge al contrasto dei furti di rame. Il filo conduttore nella soluzione di questi problemi parte sempre dal monitoraggio del fenomeno per approcciare il processo in modo integrato, avendo in mente anche il trade-off tra la sicurezza e gli altri obiettivi strategici.

Luca Comodi - Responsabile Area Network & Security Management, LABORATORI GUGLIELMO MARCONI

L'intervento ha riguardato soluzioni open source in ambito sicurezza dedicate alle aziende.

La sicurezza perimetrale è paradossalmente più facile da garantire della sicurezza del perimetro interno, tra i fattori che spiegano questa maggiore difficoltà vi è anche l'utilizzo di device personali utilizzati in ambito aziendale, per il noto fenomeno della consumerisation.

Consentire l'accesso e l'uso dei dispositivi personali ha effetti positivi su soddisfazione e produttività delle persone che lavorano in azienda, ma rende difficile mantenere gli standard di sicurezza. Possono essere proposte diverse policy per l'utilizzo sicuro di questi dispositivi, dal divieto di uso a varie forme di autenticazione, tenendo conto anche degli standard di facilità d'uso che devono essere garantiti. Lato utente, la sicurezza implica la presenza di agent sul device, che può avere impatto su velocità e funzionalità. Complessivamente, comunque, i vantaggi del BYOD sono evidenti, primo tra tutti l'ottimizzazione dei tempi.

Quali sono le linee guida per aumentare la sicurezza del perimetro interno? E' necessario partire da un monitoraggio fine degli apparati e del traffico.

E’ stato presentato un caso di studio sull’Arcispedale S. Maria Nuova di Reggio Emilia, che ha una notevole complessità e numerosità di dispositivi. L’obiettivo era la messa in sicurezza, semplificando la gestione, ma garantendo la sicurezza dei dati. Comodi ha illustrato diffusamente le soluzioni tecniche adottate per raggiungere questi obiettivi.

La conslusione dell’intervento è che BYOD e consumerisation sono esigenze che vanno affrontate con strumenti adeguati. Lo strumento proposto da L.G.M è solido e si integra con strumenti esistenti.

Giorgio Parpinelli - Director EVOLVE

L’intervento ha riguardato la steganografia, 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.

E’ una tecnica di scrittura protetta, è anche la pratica per includere dati all’interno di altri dati per renderli evidenti a terzi, un esempio normalmente utilizzato è il watermarking.

L’obiettivo di questa tecnica è di mascherare il dato all’interno di un vettore insospettabile, la staganograifa punta alla segretezza del fatto che avvenga una trasmissione. E’ stato notato che, al contrario della criptografia, non esiste una regolamentazione in materia di steganografia. L’utilizzo in ambito digitale avviene soprattutto attraverso file carrier multimediali, audio e video. Normalmente sono utilizzati messaggi i più generici possibile, per cui non sia possibile il confronto con un originale noto.

Parpinelli ha poi illustrato la network steganografia per nascondere informazioni nelle reti di telecomunicazione, con esempi sia video che audio.

Complessivamente la steganografia è una minaccia di grande portata, documentata in numerosi rapporti di intelligence. Anche in questo caso, le minacce provengono più frequentemente dall’interno. Il trend della minaccia pone gli insiders in cima alla lista dei sospettabili di attacchi, perché sono circondati da informazioni confidenziali e sensibili, hanno a disposizione dispositivi personali. Attualmente ci sono oltre 1.800 applicazioni disponibili sul web per attuare questo tipo di tecnica, la maggior parte gratuite e facilmente utilizzabili, molte dispongono anche di funzionalità di encryption. Ci si può difendere solo con un approccio integrato, che però può solo limitare i danni.

Parpinelli ha mostrato alcuni casi applicativi di utilizzo di queste tecniche in ambito criminale. Le contromisure sono ancora in fase iniziale, manca consapevolezza sui rischi e non c’è azione integrata a più livelli.

CONCLUSIONE DI DE TOMMASO, Presidente ANFoV

La sicurezza delle reti in uso è un patrimonio fondamentale per abilitare il business di qualsiasi azienda. Non solo per le informazioni che vengono gestite, ma anche per i servizi per i quali sono configurati. Pianificare, poi, la Sicurezza e la Conformità è l’unico strumento per ridurre il rischio in caso di attacco. L'enorme diffusione di applicazioni mobili, per altro, e l'adozione da parte delle aziende del BYOD (bring your own device), il consolidamento e la migrazione verso ambienti virtualizzati, e il perimetro di una rete privata che ormai non ha più una sua precisa connotazione, sono fattori scatenanti che il cybercrime conosce molto bene.
Di fronte a questi fatti ci troviamo di fronte a inconsapevolezza dei rischi, non solo da parte delle funzioni specialistiche delle aziende, ma anche da parte della politica e degli enti di controllo. Le leggi e

regolamentazioni sono infatti inadeguate e spesso non seguite; e la perdita dei dati sensibili è un fatto quotidiano.

ANFoV, CON LA COSTITUZIONE DI QUESTO OSSERVATORIO, si prefigge di creare un laboratorio dove il cybercrime e le misure di contrattacco vengano spiegate e capite, nella maniera più ampia possibile; producendo poi documentazione ad uso del Regolatore e di Autorità competenti. Ciò al fine di agevolare consapevolezza e regolamentazione appropriate.