Cyber Defence Symposium di Chiavari

Gli atti

Real Time IP Reputation: analisi «the dark face of internet» per difendere le proprie infrastrutture

Lorenzo Mazzei
Bip – Business Integration Partners

L'obiettivo di questo breve articolo è di illustrare i principali cambiamenti dovuti alla diffusione della tecnologia dell'informazione e in particolare dell'evoluzione del sistema internet, all'interno del delicato contesto della sicurezza.

Com'è noto, la diffusione di internet e l'uso dei servizi online è ormai una realtà diffusa alla maggior parte dei cittadini dei paesi industrializzati.

Le parziali difficoltà di diffusione dei computer all'interno delle famiglie sono state recentemente superate grazie alla creazione di device mobili evoluti: i tablet e gli smartphone.

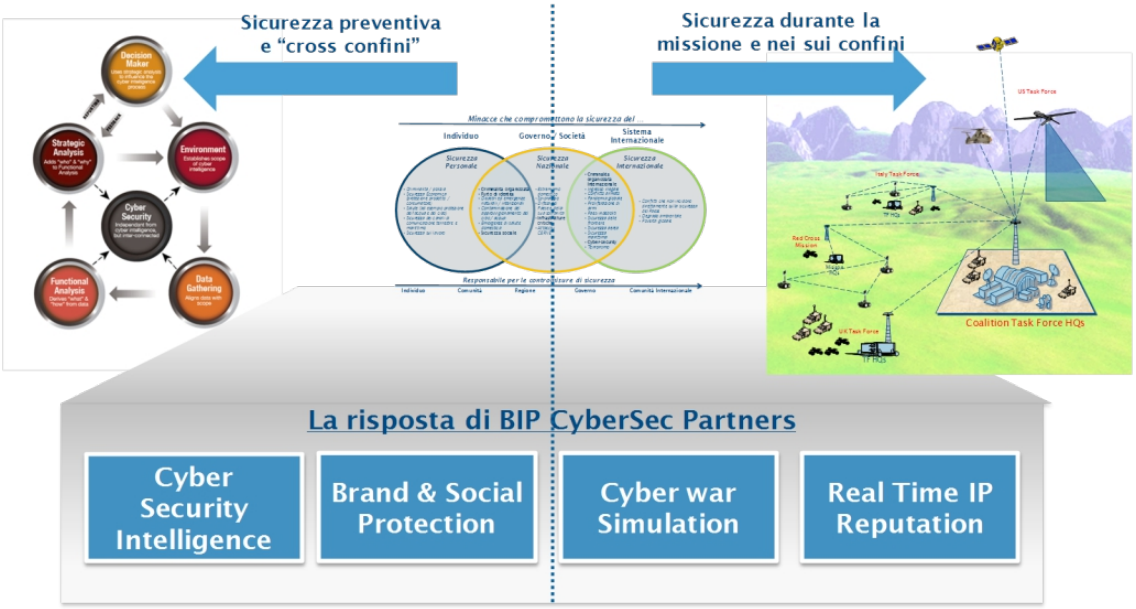
Se da un lato l'attuale sviluppo tecnologico ha permesso la diffusione di benefici in tutti i settori strategici della società, parallelamente sono emerse vulnerabilità che incidono sul livello di sicurezza di persone, organizzazioni e intere Nazioni. In particolare, negli ultimi anni si è assistito a un cambiamento nel contesto dei crimini: dai reati tradizionali, perpetrati in contesti fisici e regolamentati da leggi ben precise, si è passati a nuove forme di illecito che prevedono il ricorso al *cyberspace*, realtà favorevole alla commissione di reati e alla diffusione di nuove forme di criminalità per l'assenza di leggi, confini geografici e la possibilità di operare in anonimato. La difficoltà nell'identificazione dell'offender riduce i rischi e motiva potenziali criminali a ricorrere al *cyberspace* per svolgere attacchi

sofisticati e ben organizzati che consentono di sviluppare un volume di affari maggiore rispetto ai crimini tradizionali.

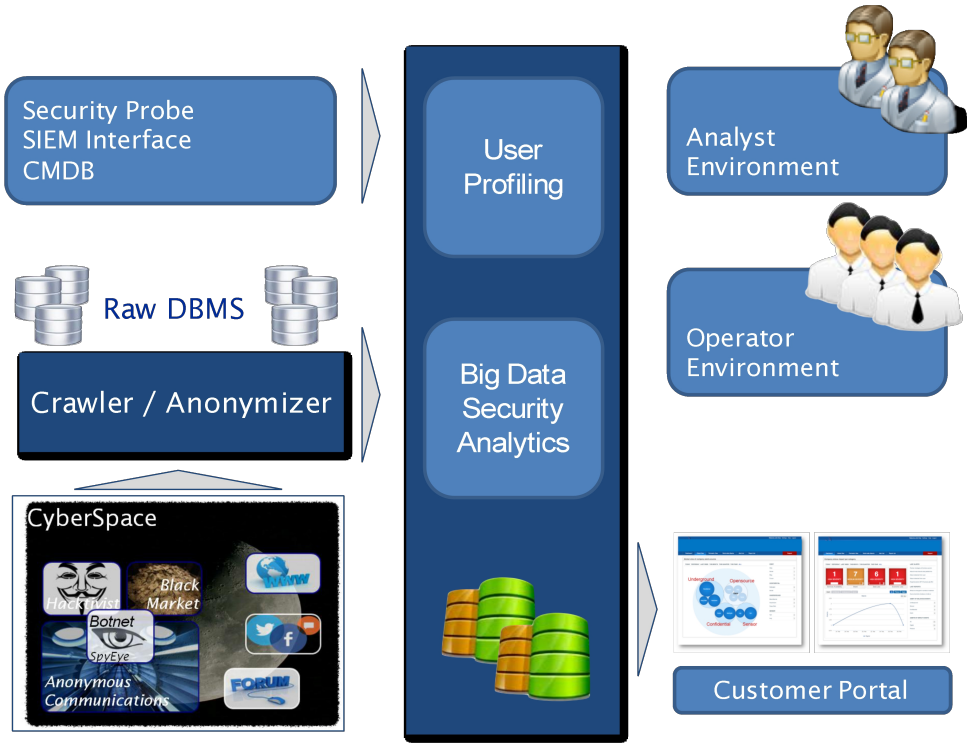
I crimini informatici rappresentano una problematica diffusa a più livelli, coinvolgendo nello stesso tempo le istituzioni pubbliche, le imprese private, fino al singolo cittadino.

Per contrastare queste nuove forme di criminalità, che compromettono la sicurezza personale, nazionale e internazionale, l'approccio più efficace consiste nell'adottare la strategia operativa propria delle agenzie governative focalizzata sull'analisi del *black market*, su attività di indagine nel *deep web* e sull'implementazione di tecnologie intelligenti per rilevare nuove tipologie di minacce provenienti dal mondo underground.

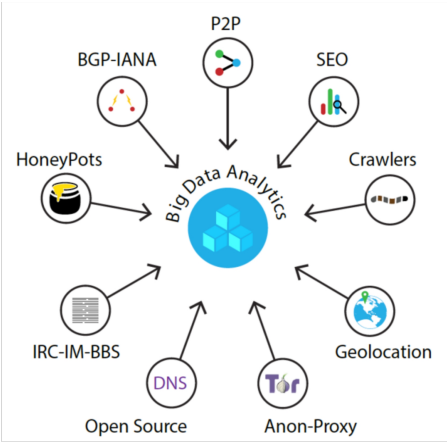
La risposta di BIP CyberSec ai crimini informatici si basa sull'adozione di un comportamento proattivo volto alla raccolta di un grande quantitativo di dati, provenienti da sorgenti classificabili in aree differenti, per contrastare minacce e innalzare il livello di sicurezza.



In particolare, attraverso la "Cyber Security Intelligence" (prevenzione e forecast di minacce attraverso la Security Analytic & User Profiling) è possibile individuare in modo preventivo potenziali azioni nocive, mediante investigazioni mirate e la creazione di identità fittizie. Tale attività è condotta previa raccolta di un grande quantitativo di dati da fonti accessibili (Open Source) e non, ovvero, dati acquisibili solo mediante sottoscrizione a servizi specifici o mediante l'invito di soggetti facenti parte di specifiche organizzazioni (Confidential).



Un altro importante servizio finalizzato a contrastare le minacce è il “Real Time IP Reputation” strumento che permette di monitorare gli indirizzi IP in tempo reale, con lo scopo di individuare e classificare le connessioni e le comunicazioni anomale, riconducibili a tentativi di attacco. Questo servizio consente alle organizzazioni di identificare e bloccare, sui servizi esposti su internet (web, posta elettronica, servizi VPN),tutte quelle connessioni provenienti da indirizzi IP classificati dal servizio di “Real Time IP Reputation” come indirizzi ad’alto rischio. Anche questo servizio si basa sulla raccolta e analisi del traffico internet: trattandosi di un servizio complesso, nel quale le tematiche di rete sono di grande rilevanza, CyberSEC collabora in questo settore con alcuni partner specializzati e focalizzati, con i quali riesce ad elaborare un volume di dati pari a circa 19 terabyte ogni giorno.



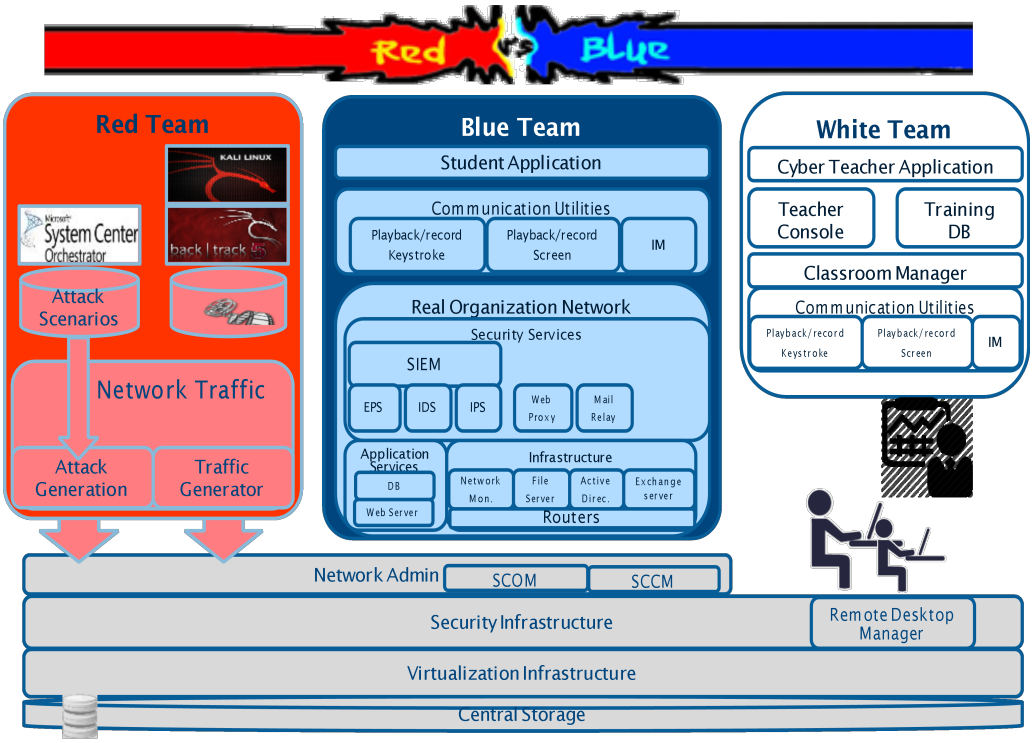
Il servizio di “Real Time IP Reputation” si basa sulla raccolta del traffico di rete da diversi service provider nei principali continenti praticamente e ha l’ambizioso obiettivo di analizzare gran parte del traffico underground, il “lato oscuro di Internet”.

Questo "lato oscuro di Internet" comprende tutto, dal traffico Deepweb (i siti web non rintracciabili tramite motori di ricerca), le connessioni peer-to-peer basate su applicazioni come IRC, la complessa e ampia rete TOR.

La tecnica di analisi di questa importante mole di traffico include anche tecniche basate sull’uso di “honeypot” (reti/sistemi trappola) nel tentativo di attirare hacker o, più frequentemente, strumenti automatizzati che attaccano le reti di computer (malware).

Ulteriori tecniche a cui è possibile far ricorso sono il “Brand Social & Protection”, volto a tutelare aziende da potenziali danni reputazionali, e la “Cyber War Simulation” che permette di creare scenari di attacco cyber, nei quali il personale dell’organizzazione deputato alla difesa da attacchi informatici, verifica il grado di capacità e competenza rispetto alle potenziali minacce di incidente. Il servizio di

Cyber War Simulation ha l'obiettivo di analizzare e creare possibili attacchi e comportamenti criminosi a danno della propria realtà aziendale, per verificare la consapevolezza e circa le proprie vulnerabilità e le competenze di difesa del personale dei Security Operation Center.



Concludendo sarà necessario che ogni paese tramite la strategie di sicurezza informatica dovrà pianificare la propria difesa e definire un percorso di preparazione.

Cyber Sec Partner quindi ha definito, come descritto sopra, i servizi per:

- Training: Cyber War Simulation
- Intelligence & Social Security
- Protection: Ip Reputation e Brand&Social Protection

Inoltre tramite il nostro team di consulenti aiutiamo le istituzioni per pianificare al meglio il processo.

Next Generation Cyber Defense: How Data Analytics Will Help Accelerate Resolution

Prakash Nagpal
Boeing

As the Internet has grown more complex and dynamic, organizations are collecting enormous volumes of data, users are connecting at tremendous speeds and there are ever-changing dynamics with millions of new devices and thousands of new applications entering the network. The Internet is hyper-connecting people with access and device freedom but with great benefits, comes petabytes of network data creating multiple vulnerabilities. As a result, today's enterprises are challenged with how to control, manage and secure their networks. 'Big data' security analytics is a new category that can help deal with these challenges through rapid incident detection and response.

In order for organizations to stay ahead, they must perform analysis on every piece of data that flows across the network and understand the data in context of everything else that is happening in the world. However, security teams are overwhelmed by the influx of data. According to a recent study by ESG Research, 29 percent of respondents note that incident detection depends upon too many manual processes. A new approach is required that draws from the richly-layered semantic web to enable machine-to-machine analysis and automated machine learning to bring deep new meaning to network activity and behavior.

Machine learning has become inherent to big data and analytics technology. The proliferation of big data and ambitious analytics projects for cybersecurity has created a need for efficient consumption of data. Machine learning provides the ability to add context to traffic and activity based on a superior understanding of data relationships, protecting virtual assets takes with a proactive approach that is easily deployed and managed. This is especially important in combating BYOD, as the multitude of devices will perpetuate the creation of an extremely diverse threat landscape.

When data visualization is combined with machine learning, security teams are able to more efficiently do their job as visual interactive analytics enrich an analyst's understanding of what's happening, why, and how to respond in real-time. Organizations that make the most of their existing security framework will be in a position to capitalize on the tremendous opportunity advanced data analytics offers. They will be able to detect problems early and shorten the time it takes to resolve the issues. Those that don't will find themselves in a perpetually reactive role where the promise of big data is not realized.

Narus nSystem' is designed to help enterprises, carriers, and governments address the very problems highlighted above. nSystem is designed to resolve threats faster by providing the context needed to understand those events and react quickly. Narus nSystem offers a holistic approach to cyber security, contextualizing and presenting data using an analytic visualization framework. This framework, based on cognitive research, was designed to present information for quick interpretation. The rich context,

powered by analytics and machine learning, allows the detection and faster resolution of previously unknown threats, thereby limiting the impact of malicious attacks. Narus nSystem fits into the existing enterprise framework, integrating with security tools and empowering perimeter defenses with enriched context (e.g., more than 500,000 application signatures).

Cyber Defence - I nuovi scenari di minaccia e le contromisure da adottare

Andrea Biraghi
Finmeccanica-SELEX ES

Nel suo intervento "Interpretare le minacce nel cyberspazio e completare la cyber defense per salvaguardare i diversi interessi nazionali", l'Ing. Biraghi ha posto all'attenzione del pubblico della conferenza numerosi temi in materia di sicurezza, offrendo al pubblico informazioni e spunti di riflessione sulla visione d'insieme, sullo scenario evolutivo, sul contesto nazionale, sul ruolo delle forze armate.

La relazione è cominciata con alcune considerazioni in merito alla digitalizzazione della società e al bisogno di proteggere le diverse infrastrutture: la digitalizzazione ha permesso lo sviluppo di nuovi servizi e ha prodotto numerose innovazioni, alcune ormai irrinunciabili, e il continuo avanzare delle innovazioni implica il ridisegno delle infrastrutture e la conseguente revisione delle strategie di sicurezza.

La parte iniziale dell'intervento ha messo in risalto alcuni dei progressi degli ultimi anni, la cui importanza è misurabile dai livelli di diffusione nella società e dalla loro quotidianità di uso da parte delle organizzazioni pubbliche, delle imprese, dei cittadini: i servizi bancari e finanziari, la sanità, la pubblica amministrazione centrale e locale, sono alcuni dei settori che stanno trasformando la propria offerta attraverso i servizi web e le tecnologie della comunicazione.

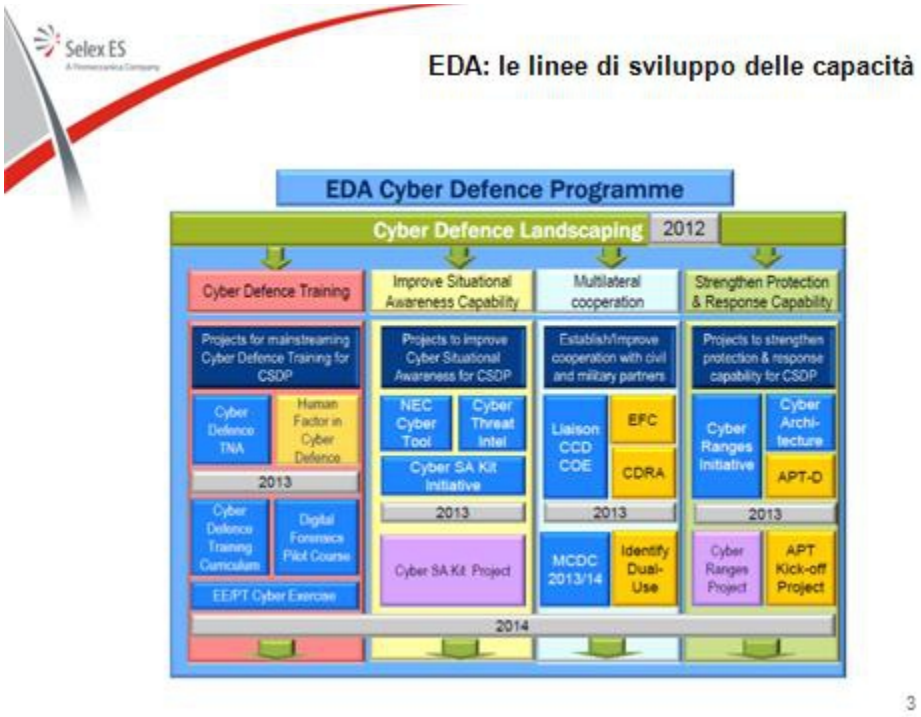
Dichiarando quanto sono indispensabili i servizi basati sulle tecnologie internet, Andrea Biraghi ha inteso affermare quanto questi debbano essere assicurati, ovvero come debbano esserne garantite la piena disponibilità, la continuità operativa, le migliori performance. Ma nel corso dell'intervento è stato anche chiarito come questi servizi tendano, quasi inevitabilmente, a dipendere da un insieme di infrastrutture dialoganti: infatti gli aspetti fondamentali di sicurezza riguardano sì, direttamente, le infrastrutture tecnologiche che consentono la pubblicazione di questi servizi web, ma in differenti casi – crescenti – gli stessi servizi dipendono dalla disponibilità di varie infrastrutture. Il cyberspazio è stato descritto come quella dimensione che consente a settori diversi di interagire: dal momento che proprio in questa dimensione sistemi differenti possono cooperare, e dalla loro interoperabilità possono sviluppare nuovo valore, l'intervento ha voluto stimolare delle riflessioni sulla sicurezza globale, sui modelli di sviluppo della cyber defence, su come estendere la cooperazione e come avvicinare il settore militare a quelli civili.

Sintetizzando il passaggio evolutivo dalla società dell'informazione alla società dell'interdipendenza, Biraghi ha evidenziato come nella società, sempre più interconnessa, servirà ampliare le competenze e le capacità tecniche in materia di cyber security, e come la protezione del cyberspazio richieda approcci largamente condivisi: l'intervento ha spiegato come la salvaguardia del cyberspace debba essere interpretata come uno sforzo congiunto, perché la sua stabilità rafforza equilibri strategici e economici, non solo militari.

Dopo aver riflettuto sulla politica internazionale sul cyberspazio e citato alcuni programmi multinazionali (in particolare gli orientamenti strategici della Commissione Europea), Biraghi ha descritto, attraverso un quadro sinottico, i principali progetti di cyber security a supporto della Difesa italiana e della NATO. Questa testimonianza ha consentito di specificare (con la duplice lettura dello scenario internazionale e nazionale) il ruolo del settore militare nel cyberspazio, le principali infrastrutture e capacità di cyber defence e, inoltre, ha messo in evidenza alcune delle attività progettuali e di fornitura di Selex ES.

L'intervento successivamente ha trattato alcune caratteristiche delle operazioni militari conducibili nel cyberspazio: oltre agli interventi a protezione degli interessi nazionali, rientranti appunto nelle strategie di cyber defence e attuabili mediante sistemi di contrasto dei possibili attacchi e servizi di prevenzione delle minacce, le capacità cyber-offensive saranno sempre più presenti nella dottrina militare. L'impiego principale dei tool offensivi si renderà utile per aggiungere efficacia alle operazioni militari, per aumentare le informazioni a disposizione sugli avversari, per poter intensificare le capacità di intelligence.

Nella parte conclusiva del proprio intervento, Biraghi ha citato la recente analisi commissionata dall'Agenzia Europea per la Difesa (EDA) sulle capacità europee di cyber-difesa, per sottolineare come lo stato attuale dei sistemi difensivi sia disomogeneo, all'interno delle forze armate europee: in prospettiva le capacità militari nel cyberspazio dovranno essere perfezionate, e i comparti della difesa europea potrebbero individuare esigenze comuni e concertare programmi, per realizzare valide collaborazioni e favorire nuovi modelli industriali. Biraghi ha commentato le iniziative europee di sviluppo delle capacità militari, comunicando l'impegno di Selex Es in ciascuno dei pilastri dei programmi internazionali: l'adeguamento dei sistemi di protezione, il miglioramento della cyber situational awareness, lo sviluppo della sicurezza condivisa, l'aggiornamento degli skill attraverso una continua formazione specialistica.



Circa gli scenari evolutivi, la relazione di Selex ES è terminata con la sintetica individuazione dei propri principali ambiti tecnologici e operativi, finalizzati a dare nuovo impulso alla cyber defence e alla protezione delle infrastrutture strategiche per la tutela degli interessi nazionali: la progettazione e sviluppo di nuovi cyber tool (difensivi/offensivi), l'integrazione delle azioni di rilevamento, contrasto e contenimento con le tecniche di intelligence e con nuovi sistemi di allarme sulle minacce, la realizzazione di nuove modalità integrazione / interoperabilità dei SOC e CERT.

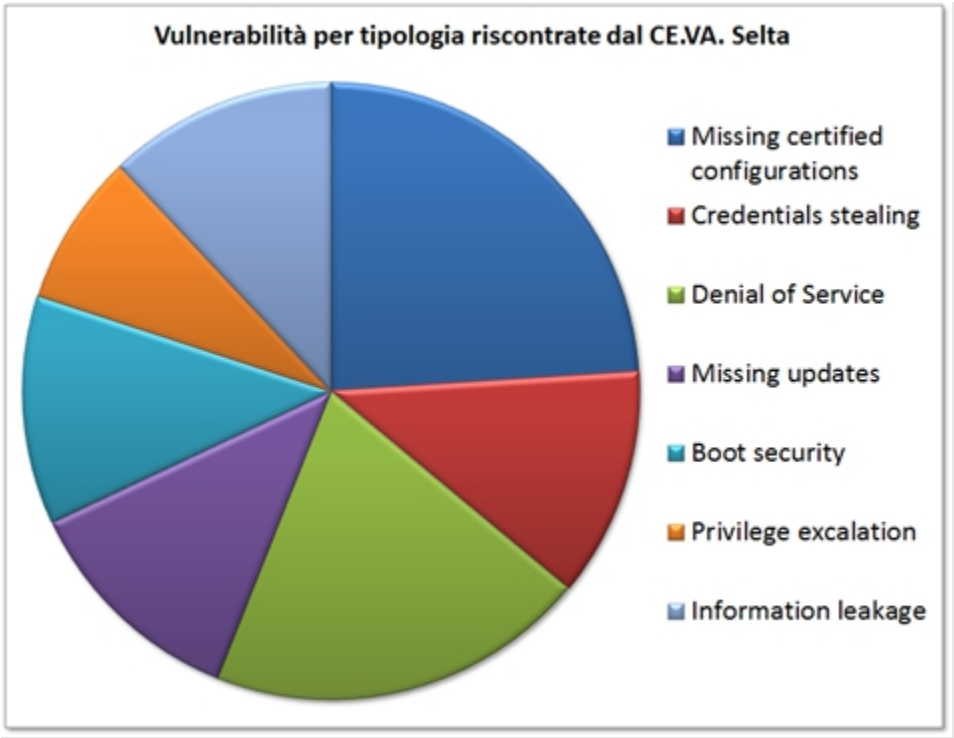
SELTA – Alcune offerte per la Difesa: Common Criteria e Carrier Ethernet

Giacinta Santo
SELTA

La Business Unit Defence & Cyber Security della SELTA S.p.A. dispone di **laboratori CE.VA./LVS** per la valutazione della sicurezza informatica di sistemi/prodotti secondo gli standard ISO 15408 (Common Criteria) e ITSEC.

Il laboratorio CE.VA. è accreditato dalla Presidenza del Consiglio dei Ministri - Dipartimento Informazioni per la Sicurezza ad operare secondo il D.P.C.M. 11/04/2002, e successive modifiche, "Schema Nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT" che trattano dati classificati. Il laboratorio LVS è, invece, abilitato dall'OCSI del Ministero dello Sviluppo Economico ad operare secondo lo "Schema Nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT" inserito nel D.P.C.M. 30/10/2003.

I laboratori SELTA operano seguendo i suddetti standard dal 1997: da allora hanno eseguito la consulenza e l'assistenza completa (per numerosi clienti) nella produzione della documentazione per la valutazione ed hanno concluso positivamente la valutazione di circa venti, tra sistemi e prodotti da livelli bassi a livelli medio-alti di garanzia. In questo lungo arco di tempo sono state rilevate e risolte vulnerabilità di differenti tipologia ed impatto, come illustrato nel seguente grafico.



Nel corso della propria esperienza i laboratori hanno verificato che l'efficacia dello standard è stata talvolta sminuita dall'uso puramente commerciale della certificazione, comportandone una perdita di vigore. In tal senso, i laboratori SELTA stanno cercando di veicolare il nuovo approccio del Common Criteria Recognition Arrangement, secondo il quale si rende opportuno definire problemi di sicurezza (Protection Profile collaborativi) per specifiche tematiche tecniche all'interno di gruppi di lavoro eterogenei (ad es. Industria, mondo Accademico, ecc.) in ambito **Infrastrutture Critiche Nazionali**.

Le attività svolte dai laboratori SELTA consistono, in parte, proprio nelle verifiche di compliance a standard e protocolli di sicurezza che nel "Piano Nazionale per la protezione cibernetica e la sicurezza informatica" (D.P.C.M. del 27/01/2014) vengono citate nell'Indirizzo Operativo 7 quale strumento fondamentale per garantire la protezione cibernetica e la sicurezza informatica dei sistemi e delle reti, a livelli qualitativi omogenei ed elevati.

Nell'ambito della terza edizione del **Cyber Defence Symposium**, svoltosi gli scorsi 13 e 14 maggio ed organizzato dalla Scuola Telecomunicazioni delle Forze Armate di Chiavari, SELTA ha presentato, in sintesi, l'utilità dell'applicazione degli standard citati non solo come riferimento per le valutazioni e la pianificazione dei test di sicurezza, ma anche come modello di sistemi e prodotti ICT utile nella progettazione della sicurezza degli stessi. L'intervento ha evidenziato quelli che sono gli impatti del nuovo approccio alle compliance sulla realtà nazionale ed ha descritto come SELTA sta applicando il

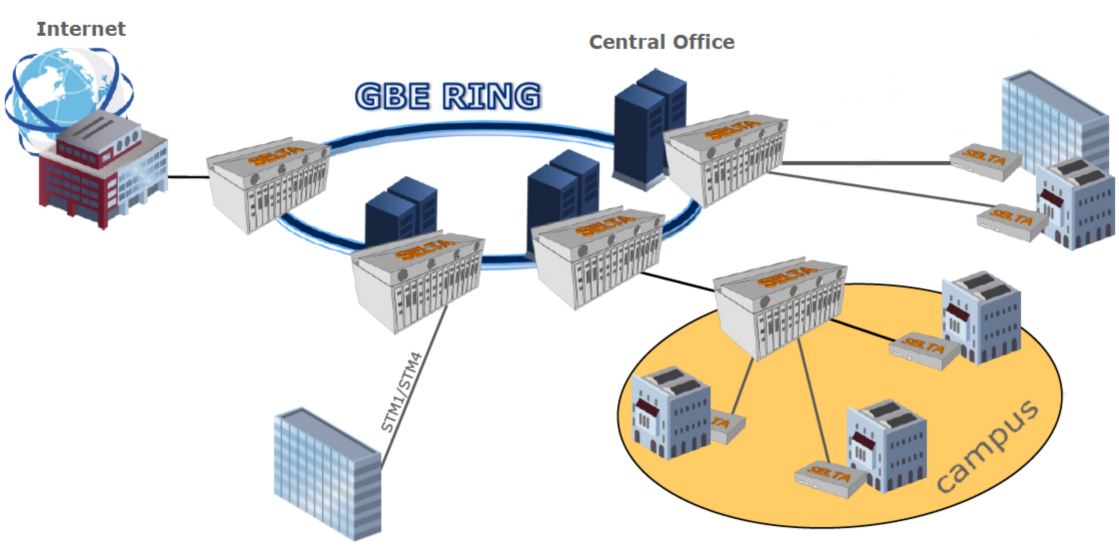
modello delle Technical Communities nella definizione del problema di sicurezza per infrastrutture critiche nazionali.

Nel corso dello stesso Simposio, è stato messo a disposizione di SELTA uno spazio espositivo attraverso il quale il personale dell'Azienda ha avuto l'opportunità di presentare le attività di pertinenza ed i segmenti di mercato di SELTA, Gruppo Industriale che opera **non solo nel mondo della Cyber Security, ma anche in quelli inerenti all'ICT, l'Elettronica e le Telecomunicazioni**, offrendo alla propria Clientela **soluzioni e servizi orientati alla sicurezza**. In particolare, la sopracitata Business Unit è inoltre fortemente attiva nel campo dei servizi di consulenza ICT, nella realizzazione di infrastrutture sicure di comunicazione e nei servizi di assistenza tecnica, sistemistica ed operativa.

Lo stand di cui sopra è stato utilizzato da SELTA anche per offrire una panoramica dei prodotti che la stessa sviluppa nel campo delle **Reti di Accesso** e che possono trovare un positivo riscontro di utilizzo anche per il networking della Difesa. Tali prodotti spaziano dai dispositivi Access Multiplexers (DSLAM) alle soluzioni Carrier Ethernet. Entrando nel merito di queste ultime, SELTA ha sviluppato una famiglia di apparati (**Piattaforma Carrier Ethernet**), la cui principale funzionalità è quella di sovraperformare il trasporto di connettività nelle tratte di rete costituite da rame. Attraverso tali dispositivi è possibile realizzare soluzioni altamente scalabili, ma anche circoscritte ad una singola tratta: la Piattaforma consiste, infatti, sia in apparati di tipo centralizzato (rack e schede di rete) che in apparati di tipo stand-alone periferici (modem).

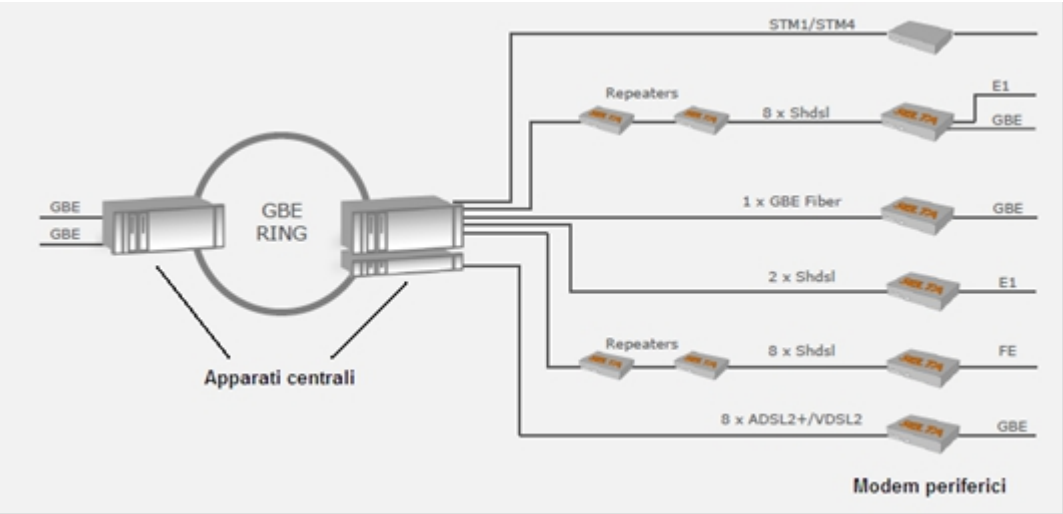
Al giorno d'oggi, lo sviluppo di soluzioni a larga banda è spesso accompagnato da interventi infrastrutturali non sempre possibili (o comunque di complessa fattività) e soprattutto da investimenti economici molto onerosi che, poi, non sempre sono giustificati dai requisiti definiti in fase di progettazione. La disponibilità di una rete di trasporto in rame, invece, è molto diffusa e scarsamente utilizzata, anche perché non sfruttabile per le esigenze tipiche delle reti di nuova generazione.

Nei **contesti militari inerenti al mondo della Difesa**, la Piattaforma Carrier Ethernet si inserisce come soluzione per la realizzazione di dorsali Ethernet, in maniera tale da raccogliere flussi di traffico in aree ove disponibile doppino telefonico in rame, all'interno di un compound (ad es. palazzine distaccate, uffici tecnici territoriali, pluralità di depositi, magazzini, aule, alloggi, procure, sacrari ed ordinariati militari, ecc.), e le cui distanze richiederebbero obbligatoriamente la connessione tramite fibra ottica.



La soluzione Carrier Ethernet di SELTA consente di realizzare anelli in fibra ottica con modulazione di tipo CWDM (Coarse Wavelength Division Multiplexing) garantendo ridondanza, resilienza ed affidabilità, per configurazioni, con differenti funzionalità, capaci di rendere disponibile la rete Ethernet da dorsali centrali/metropolitane fino alle postazioni remote. La capillarità della rete Ethernet permette, ad esempio, la realizzazione di soluzioni tipiche delle Smart Cities in cui la rete è utilizzata per veicolare il traffico proveniente dal monitoraggio delle aree sensibili alla sensoristica per la regolazione del traffico, dalla diffusione di contenuti multimediali all'analisi delle condizioni climatiche.

La Piattaforma si presenta pertanto come soluzione ottimale per realizzare dorsali Ethernet, in maniera tale da raccogliere flussi di traffico in aree ove disponibile doppino telefonico in rame (all'interno di compound) ed in cui le cui distanze richiederebbero obbligatoriamente la connessione tramite fibra ottica. A livello di prestazioni, tale soluzione copre distanze **fino a 4 km** e porta la connettività **fino a 45 Mbps** su doppini in rame (bonding a 8 coppie).



I vantaggi dell'impiego di tale soluzione sono:

- **rapidità dell'iter autorizzativo**, per l'impiego dei dispositivi, fra gli Enti della Difesa coinvolti (ad es., Geniodife, ecc.);
- semplicità di **realizzazione della soluzione**, senza il bisogno di investimenti ed interventi progettuali/realizzativi all'infrastruttura;
- **installazione rapida** (numero ridotto di parametri di configurazione) **e completamente trasparente all'operatività** (no interruzioni di essa);
- **non sono necessari corsi di formazione** del personale impiegato per la configurazione e gestione degli apparati, **né costi né attività di manutenzione ordinaria** dei dispositivi stessi;
- la soluzione può essere smontata e riutilizzata in altro sito/contesto, **salvaguardando l'investimento sostenuto**.

Gestione delle minacce informatiche nell'ICT bancario

Amedeo Vitigliano Stendardo

I gruppi creditizi assumono un ruolo di fondamentale importanza nel sistema finanziario: il gruppo è infatti la forma privilegiata dell'impresa di rilevanti dimensioni e consente di operare in modo efficiente, più competitivo e meno rischioso in una pluralità di mercati e settori di attività.

Anche la struttura del sistema bancario italiano ha attraversato nell'ultimo decennio una fase di notevoli cambiamenti dovuti principalmente a fusioni ed acquisizioni tra banche nazionali.

L'interesse economico per una diversa distribuzione della dimensione delle banche italiane è nato dal fatto che l'evoluzione della struttura del mercato poteva portare a cambiamenti nelle politiche di credito delle banche con effetti di razionamento specialmente per le piccole e medie imprese (PMI).

Il contesto europeo in cui il sistema bancario italiano si trova ad operare pone quindi la necessità di un continuo confronto con i gruppi esteri riguardo alle modalità operative, alla dimensione e alla localizzazione delle strutture organizzative, al livello e alla tipologia di informatizzazione, soprattutto alle varie normative vigenti in ogni paese.

I gruppi italiani operano prevalentemente nel settore Retail Banking, mentre i gruppi esteri presentano un'operatività più estesa anche ai settori Corporate and Investment Banking e Private Banking. Inoltre, più del 50% dei gruppi esteri svolge altre attività - in aggiunta a quelle più propriamente bancarie - che spaziano dal Leasing al Factoring, dall'Insurance al Consumer Finance, dal Real Estate al Wealth Management, con percentuali dal 2 al 20% dell'operatività complessiva. I gruppi esteri hanno una maggiore concentrazione sia di banche sia di strutture informatiche nell'Europa centrale, in Asia e nel Resto del Mondo, mentre i gruppi italiani una maggiore presenza nell'area Mediterranea e nell'Est Europa.

Le strutture informatiche dei gruppi esteri sono quasi totalmente attestate presso una componente bancaria dello stesso gruppo, mentre quelle dei gruppi italiani risultano in maggioranza affidate a una componente non bancaria del gruppo o a una società esterna. Il modello organizzativo della "fabbrica ICT" adottato dal 60% dei gruppi nazionali è quello centralizzato, a fronte di un orientamento prevalente dei gruppi esteri per strutture centralizzate con alcuni centri di competenza o per varie forme di decentramento.

Tali diversità condiziona ovviamente le modalità operative adottate da ogni gruppo e, di conseguenza, soprattutto le scelte in campo ICT e i connessi costi.

Le quote maggiori di spesa ICT vanno prioritariamente ai "servizi da terzi" e al "personale interno"; seguono quelle per il "software" e per l'"hardware". Per i gruppi esteri la quota maggiore è rappresentata dal "personale interno", in coerenza con il modello di insourcing prevalentemente adottato per la gestione dei servizi ICT, mentre per quelli italiani sono i "servizi da terzi" che assorbono la quota prevalente, in linea con il maggior ricorso a forme di outsourcing.

Confrontando le scelte tecnologiche e gli indirizzi, in termini di investimenti, per l'innovazione, sostanziali differenze si riscontrano laddove si prenda in considerazione la nazionalità della capogruppo: i gruppi italiani dichiarano una percentuale media del 7% del cashout 2013 per investimenti in tecnologie innovative, contro un 20% segnalato dai gruppi esteri. Gli ambiti tecnologici ove si sono concentrati i maggiori investimenti sono il VoIP, la Business intelligence, la virtualizzazione e la Green IT, utilizzati prevalentemente a supporto delle esigenze interne. Una parte significativa degli investimenti in programma è invece rivolta ai servizi alla clientela e riguarda soprattutto le tecnologie del WEB 2.0, del Mobile, della Business intelligence e del Contactless; di sicuro interesse risulta, sia per le funzioni interne sia per i servizi alla clientela, anche il Cloud computing.

Le politiche di sviluppo dei canali di contatto con la clientela sono fortemente condizionate dal tipo di attività del gruppo. I canali valutati maggiormente in crescita sono l'Internet banking e il Mobile banking, seguiti dall'ATM-Self Service, mentre risultano stabili, in prevalenza, il Call Center e lo sportello, quest'ultimo in diminuzione.

Per far fronte ai rischi connessi con l'utilizzo dei canali telematici - con riguardo in particolare al furto di identità - i gruppi bancari, a prescindere dalla nazionalità della capogruppo, curano la diffusione presso la clientela di norme comportamentali attraverso la pubblicazione di avvisi sui propri portali o siti Internet; è inoltre in programma, da parte di tutti i gruppi italiani e della maggioranza dei gruppi esteri, l'introduzione di specifiche linee guida indirizzate alla sola clientela che opera su Internet.

Oltre a queste iniziative, la quasi totalità dei gruppi ha adottato al proprio interno specifiche contromisure organizzative e policy di sicurezza, prevedendo anche strutture organizzative permanenti dedicate allo scopo. Tra le misure di sicurezza, generalizzata è l'adozione di tecniche di "autenticazione forte" della clientela, di procedure codificate in risposta alle frodi informatiche, di meccanismi di controllo sull'operatività dei clienti mirati ad una tempestiva individuazione delle frodi. Diffuso è anche il ricorso a forme di collaborazione con le forze dell'ordine, finalizzata alla

prevenzione/repressione delle frodi (Polizia di Stato, Guardia di Finanza e Direzione Investigativa Antimafia), e a piani di formazione del personale adibito ai call center a supporto della clientela.
Tecniche (come la scansione periodica del Web e l'analisi dei log) utili per l'individuazione di possibili azioni fraudolente, quali la simulazione del sito Internet del gruppo, sono utilizzate da circa l'80% dei gruppi bancari.
Quindi la grande diffusione dei servizi ICT per le banche oramai è tale che la loro complessità richiede l'integrazione anche con attente analisi di gestione dei rischi.
Grazie alla sua ampiezza, il mercato finanziario sintetizza le esigenze di sicurezza provenienti da mercati diversi, come l'industria (protezione dei beni, protezione di persone), i servizi ICT (continuità del servizio, la sicurezza dei dati), i media (protezione del marchio, la sicurezza dei pagamenti), il pubblico (gestione delle crisi).
Allo stesso tempo, i servizi ICT bancari sono oggetto di una vasta gamma di minacce e dei rischi in evoluzione, a volte eseguiti dalla criminalità organizzata con l'obiettivo di attaccare in generale il sistema finanziario.
Il numero di frodi e attacchi realizzati tramite servizi ICT è in crescita e il furto di identità è il secondo più denunciato. Frodi finanziarie, infezioni da malware, denial of service, password sniffing e defacement di siti Web sono in crescita, anche se le perdite medie a causa di incidenti di sicurezza stanno riducendo grazie ad un aumento generale di sensibilizzazione alla sicurezza e per le soluzioni di sicurezza adottati. Le conseguenze dovute alla perdita di dati non sono limitati alla dimensione economica delle frodi ma possono avere impatti sociali come dimostrato da Wikileaks.
Le banche e le istituzioni finanziarie in generale devono monitorare con unità di sicurezza interne dedicate all'evoluzione delle minacce ICT al fine di attivare misure di sicurezza idonee volte a prevenire e proteggere questi tipi di attacchi che possono ridurre la fiducia dei servizi gestiti.
In questo contesto la Sicurezza ICT implementa i processi, i controlli, le architetture, soluzioni e servizi di monitoraggio volti a ridurre i rischi dovuti ad eventi di Cyber Crime, soprattuto deve proteggere l'azienda e i valori del Gruppo.
La crisi economica iniziata nel 2008 ha imposto nuovi valori ai gruppi creditizi in generale, ovvero la protezione delle informazioni, la loro gestione, con costi minori. Perchè la protezione concreta delle informazioni è direttamente connessa con il valore reputazionale dell'istituto bancario, messo in distussione soprattutto in periodi di crolli finanziari. Tutto ciò, chiaramente, non prescindendo dalla necessità di essere trasparente.

L’era virtuale e, con questa, l’adozione di servizi on-line hanno modificato anche i concetti di perimetro della banca, di interesse alla sicurezza, che si allarga fino al device del cliente nel momento in cui questo è collegato in home banking.

Quindi, ogni strategia di sicurezza e ogni analisi di rischio non può prescindere dal tener conto anche del laptopo del cliente, con il quale questi compie transazioni che potrebbero mettere in pericolo l’immagine dell’azienda se, durante una di queste, un malware si insinua, non solo ma viene messo in pericolo l’istituto di credito dalla stessa condotta del cliente se questo è legato ad organizzazioni criminose di diverso tipo che impongono illecite movimentazioni di danaro. Come parte del perimero della banca, così, sono tutti i player che operano per la banca, persone e società, sui quali, a divcerso livello, è necessario informarsi prima.

La sicurezza bancaria e le giuste analisi dei suoi rischi sono quindi molto importanti perchè la natura stessa della banca la vuole come centro di interessi particolari che si incrociano tra di loro, nell’era in cui l’interesse economico-monetario è direttamente collegato con i dati personali, la cui riservatezza e protezione va sempre garantita e protetti pure in presenza di necessarie misure di monitoraggio.

Anatomia di un CERT
Un quadro di riferimento della funzione di prevenzione e gestione delle emergenze Cyber

Toto Zammataro

Il CERT (Computer Emergency Response Team) è il gruppo deputato alla protezione di specifici persone/asset/interessi, che vengono definiti "Constituency", dagli incidenti legati all'ICT.
Il tema del CERT ha subito una evoluzione molto ampia negli ultimi 25 anni. In particolare l'acronimo, che è rimasto nel gergo come sinonimo del team di gestione incidenti, è stato tecnicamente sostituito dal più specifico acronimo CSIRT (Computer Security Incident Response Team), in modo da rendere evidente il tipo di emergenze che questo gruppo è chiamato a gestire seguendo un processo predefinito: il processo di Gestione Incidenti. A seguire della sofisticazione delle minacce e dell'aumento esponenziale delle attività di attacco seguite dall'espansione di Internet, i CERT più maturi sono evoluti aggiungendo servizi complementari al processo di Gestione Incidenti. Questi servizi, come la threat intelligence, la malware analysis, il supporto alla ricerca accademica e/o industriale, hanno permesso di focalizzare il CERT sulla gestione degli incidenti ad alto impatto, lasciando al SOC la gestione degli incidenti "ordinari". Questa evoluzione ha portato alcuni esperti a dare nuovo significato all'acronimo, sostituendo Response con Readiness. I CERT più maturi ed avanzati sono ora impegnati in prima linea nel preparare la propria Constituency, nell'identificare le minacce più subdole e nascoste (i.e. *Spear Phishing, Advanced Persistence Threat, State Sponsored attacks, ...)* e, naturalmente, nel supportare nella gestione degli incidenti più gravi.

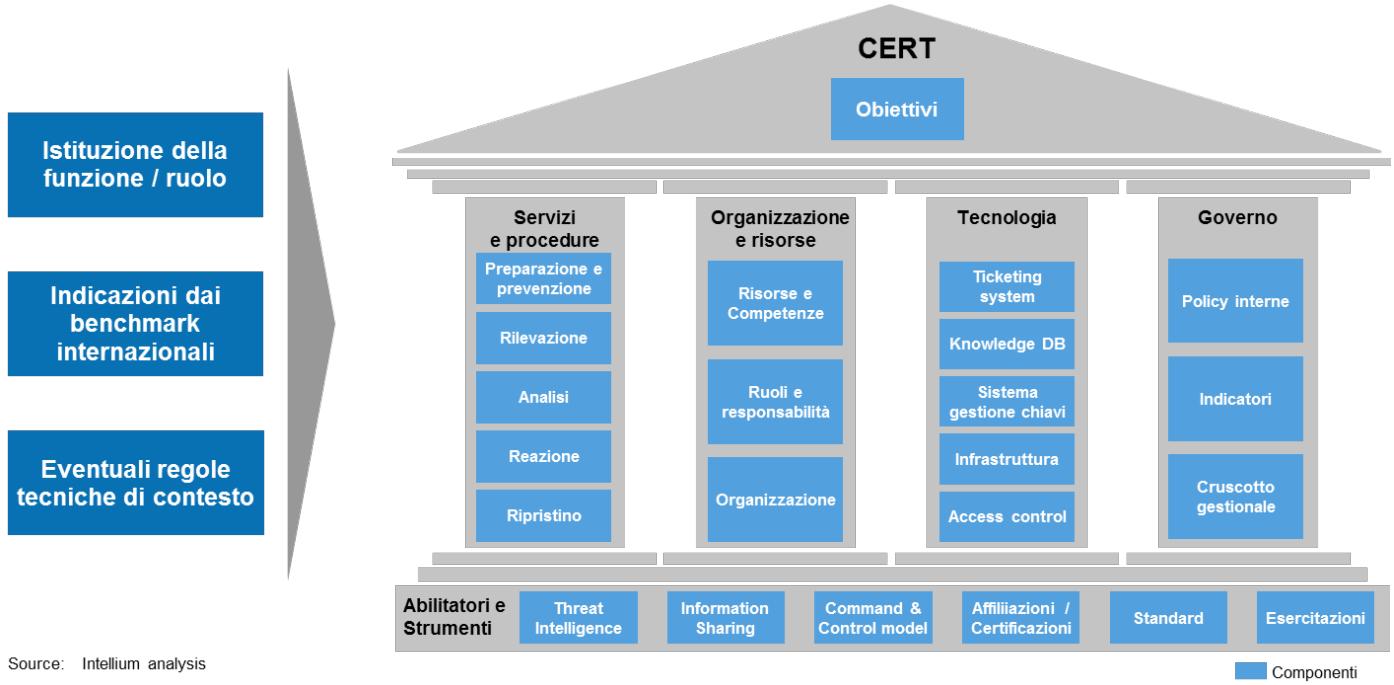
Nei casi di incidente il CERT agisce da coordinatore delle comunicazioni sia interne alla Constituency che verso gli attori esterni necessari per preparare e governare il processo di risposta. Gli attori esterni possono essere di tre classi:

- Interlocutori istituzionali e governativi: sono una fonte preziosa di informazioni e sono essenziali per il supporto durante la mitigazione dell'incidente. In questa classe esistono diversi enti, come ad esempio il CERT Nazionale, il CERT-PA, il CERT Difesa, il CNAIPIC, …
- Interlocutori nazionali: tra gli attori di questa classe sono da annoverare i CERT delle aziende private, le aziende di telecomunicazione, l'accademia, gli enti operativi a supporto delle emergenze non cyber (es. VV.FF., Protezione Civile, Ospedali, …)

- Interlocutori internazionali: oltre ai singoli CERT e le aziende estere da contattare in caso fossero coinvolte in uno specifico incidente, gli interlocutori internazionali più importanti sono i gruppi di CERT, quali il FIRST, Il Trusted Introducer, e l'ENISA. Essi, in modo diverso e con un diverso grado di fiducia, costituiscono la fonte principale per
  - confrontare e valutare l'operato del CERT nella gestione incidenti,
  - ricevere ed inviare informazioni riservate ed allarmi alla comunità internazionale

Il modello operativo del CERT è specificato in funzione del ruolo previsto nella Constituency e si basa su sei componenti fondamentali:

1. Obiettivi
2. Servizi e procedure
3. Organizzazione e risorse
4. Tecnologia
5. Governo
6. Abilitatori e strumenti



Source: Intellium analysis

Queste componenti, che ogni CERT deve personalizzare e fare propri, sono necessari per fare funzionare correttamente il team durante la gestione degli incidenti. Per ciascuno di essi è importante

specificarne le caratteristiche ed evidenziare quali errori sono da evitare nella loro definizione e messa in esercizio.

1) Obiettivi

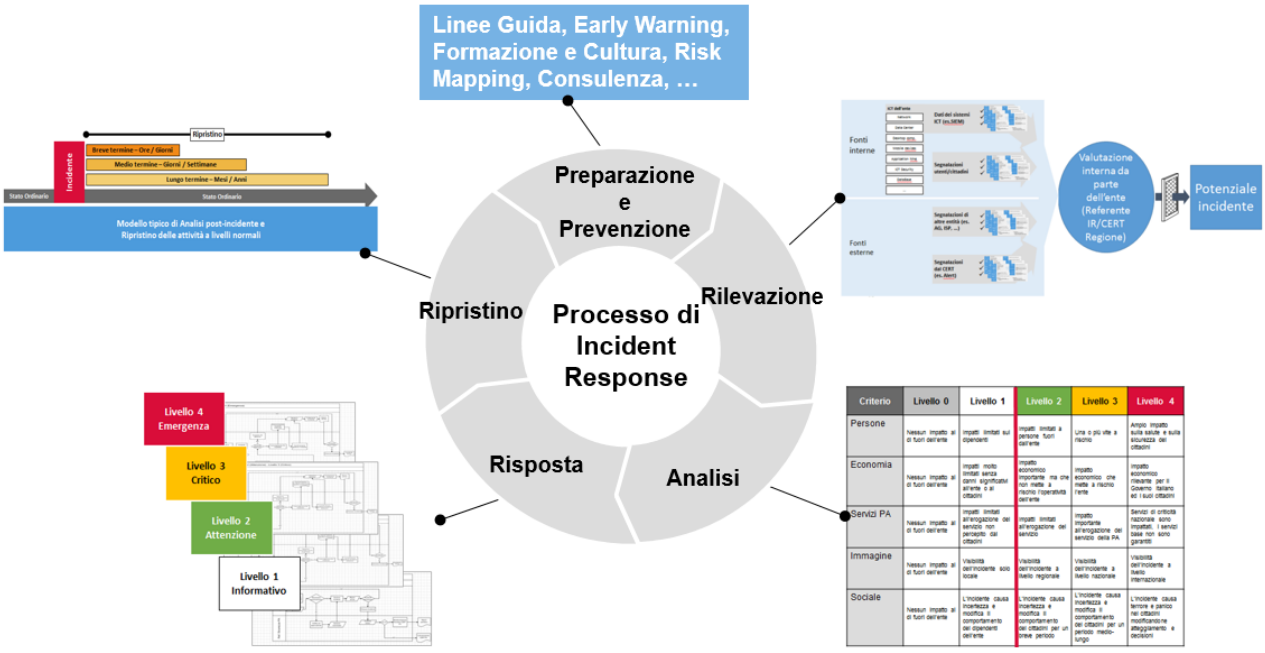
L'obiettivo principale di un CERT è di agire da punto di riferimento nella prevenzione e gestione degli incidenti Cyber: questa affermazione generica deve essere contestualizzata e comunicata all'interno (e spesso anche all'esterno) della Constituency; per specificare meglio gli obiettivo, può essere prodotta una lista che li raccolga, come ad esempio:

1. Prevenire e/o ridurre gli impatti di incidenti Cyber
2. Stabilire un modello di ruoli e responsabilità per l'Incident Response
3. Raccogliere e controllare le informazioni per la prevenzione e la risposta agli incidenti
4. Facilitare la consapevolezza sui temi di Cyber Security e la condivisione delle informazioni
5. Stabilire il modo formale per scalare da attività operative (SOC) a gestione incidente (CERT)
6. Identificare in modo formale gli incidenti Cyber per la Constituency

La diffusione continuativa degli obiettivi del CERT permette a tutti i diversi attori di capire quali siano le tipologie di servizio che il CERT fornisce. Questi ultimi possono essere diversi, ma il processo di Incident Response non puo' mancare. Il dettaglio di quali siano il servizi erogati dal CERT è l'argomento del prossimo punto.

2) Servizi e procedure

Il processo di Incident Response è il processo chiave che è ragione dell'esistenza di un CERT e specifica chiaramente le fasi, i ruoli e le responsabilità richieste agli attori principali



Questo processo viene normalmente declinato nelle cinque fasi di:

- Preparazione e prevenzione: all'interno di questa fase sono contenuti normalmente anche i servizi opzionali/evoluti del CERT, come ad esempio la consulenza, il Risk Mapping, il supporto per la gestione dei dati personali, lo studio di malware e virus, lo sviluppo di codice sicuro, la formazione, … Quello che normalmente è sempre presente sono il servizio di Early Warning (bollettini di sicurezza) e la pubblicazione delle linee guida di sicurezza (di concerto con altri enti/uffici aziendali) necessarie per chiarire il livello minimo di sicurezza previsto all'interno della Constituency (e, di conseguenza, gli SLA attesi che saranno monitorati dalla componente di Governo)
- Rilevazione: la fase di rilevazione costituisce l'avvio della gestione incidente. Senza una codifica corretta delle fonti e dei segnali (interni ed esterni) il CERT non è in grado di rilevare gli incidenti, di fatto rendendolo inutile. E' la fase del processo più delicata e su cui lavorare in modo prioritario durante la costruzione del CERT. Durante la rilevazione si svolge anche uno dei compiti più sensibili del CERT, cioè la classificazione dei dati per stabilirne la loro diffusione. Lo standard di riferimento adottato dalla comunità dei CERT è il TLP (Traffic Light Protocol). E' in questa fase che si

raccolgono i frutti di una adeguata preparazione, dopo avere posto in essere tutti i sensori utili per evidenziare le anomalie provenienti dai sistemi interni, dalle fonti esterne o dal gruppo del CERT che interpreta i segnali del servizio di Threat Intelligence.

- Analisi: a fronte della rilevazione di un evento, deve essere svolta l'analisi per identificare chiaramente la classificazione dell'incidente. In questo caso l'adozione di una matrice di classificazione è lo strumento chiave per distinguere gli incidenti "ordinari" (che vengono gestiti nel *day-by-day* dal SOC – Security Operation Center) da quelli che possono avere un impatto più significativo e che dovranno essere gestiti dal CERT. Le classificazioni ad alto impatto (es. Livello 2,3,4 dell'esempio) scateneranno la fase successiva.
- Risposta: contro-intuitivamente questa è la fase del processo di Incident Response più semplice da fare funzionare correttamente, in quanto deve essere proceduralizzata e continuamente verificata. Le procedure, come in ogni processo di miglioramento continuo, saranno sempre più efficaci ed aderenti ai bisogni della Constituency mano a mano che verranno utilizzate. A seconda del tipo di organizzazione scelta, il CERT sarà semplicemente il coordinatore delle diverse azioni previste o, in casi più operativi, agirà autonomamente per specifiche attività (es. comunicazione con i media, comunicazione con l'autorità giudiziaria, definizione delle misure tecniche di contenimento, …)
- Ripristino: l'ultima fase del processo prevede il rientro ad uno stato di normalità; è l'occasione in cui si "tirano le somme" e si analizza nel dettaglio la risposta che è stata data all'emergenza; quanto rilevato viene poi mantenuto nel "knowledge DB" ad uso del personale che sarà coinvolto in futuro in accadimenti simili.

3) Organizzazione e Risorse

Parlando di personale, le risorse umane del CERT dovranno essere scelte sulla base di una selezione basata sulle caratteristiche personali, sulle competenze e dopo l'esito positivo di *background check*. Il lavoro all'interno di un CERT prevede carichi di stress anche per periodi prolungati: scegliere persone adatte per gestire queste condizioni di pressione è uno dei fattori vincenti del CERT. Oltre a questa caratteristica di base (Capacità di gestire lo stress) qui di seguito un elenco di caratteristiche e competenze importanti per questo tipo di personale:

Caratteristiche personali

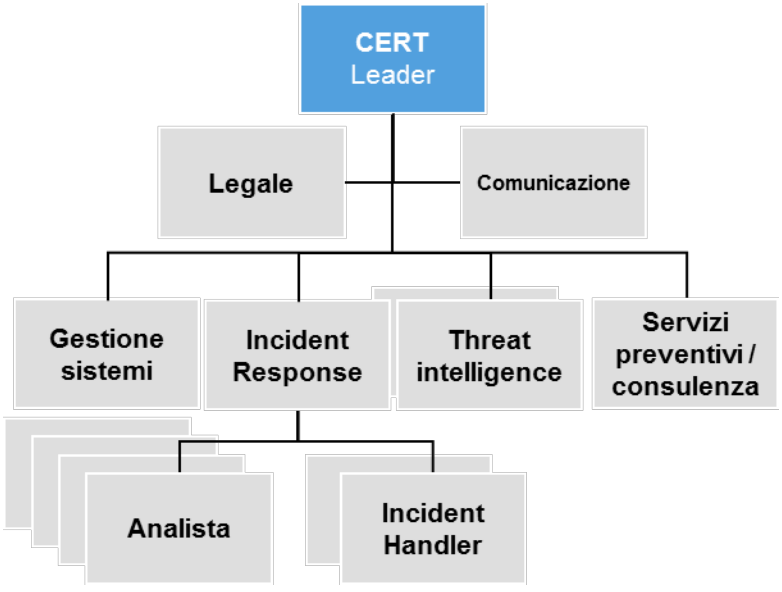
- Integrità
- Capacità di comunicazione scritta ed orale
- Diplomazia
- Capacità di seguire policy e procedure
- Capacità di contribuire al gruppo di lavoro
- Comprensione dei propri limiti

- Problem solving
- Capacità di saper gestire il proprio tempo
- Attenzione ai dettagli ed ai segnali deboli
- Capacità deduttive ed analitiche

Competenze

- Buone competenze sui fondamenti dell'ICT
- Comprensione dei principi di sicurezza ICT
- Comprensione delle vulnerabilità e delle debolezze delle componenti hw/sw/human della sicurezza
- Storia di internet e della sua evoluzione
- Rischi di sicurezza delle informazioni
- Protocolli di rete
- DNS
- Servizi ed applicazioni di rete
- Contromisure tecnologiche di sicurezza
- Sicurezza dei sistemi operativi
- Conoscenza e capacità di identificare tecniche di intrusione
- Crittografia: caratteristiche, debolezze, strumenti
- Capacità di programmare

Identificate le figure adatte con il corretto mix di competenze tecniche, legali e di relazione, la struttura del CERT può essere rappresentata dal seguente schema:



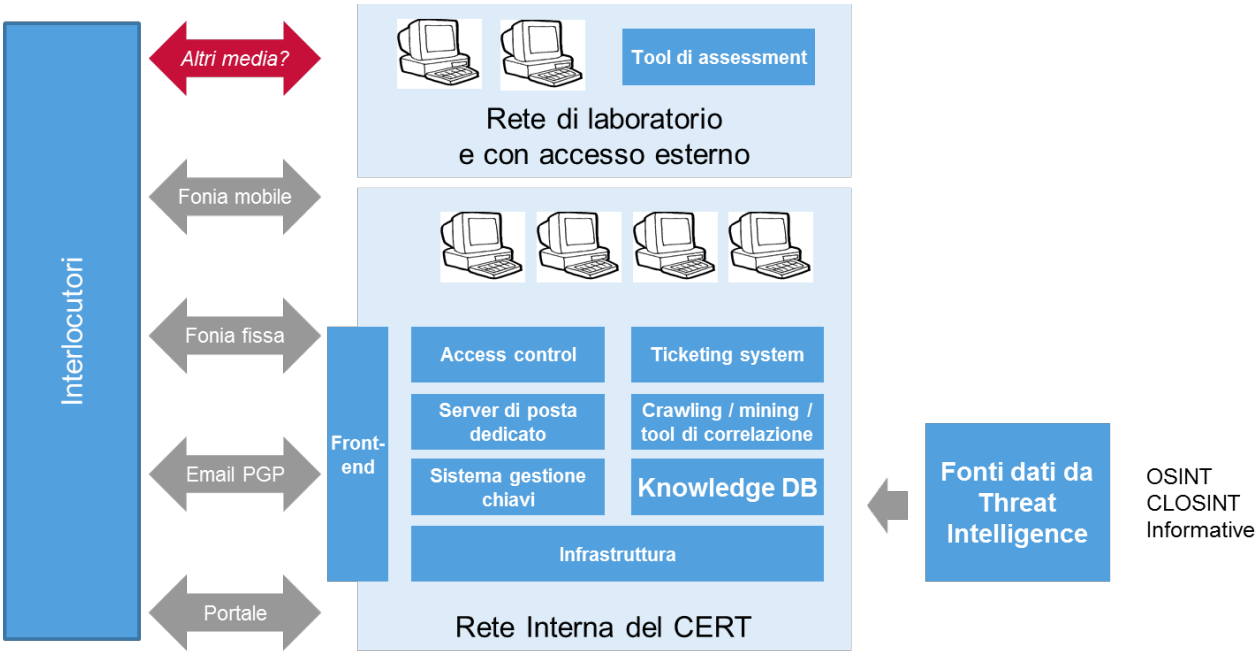
La dimensione del team di lavoro dipende dalla quantità di attacchi/incidenti che hanno come target la Constituency e può variare da poche unità a team di 20 e più persone.

Dipendentemente dalla Constituency e dagli obiettivi possono essere previsti turni 24x7 per gli analisti e la reperibilità per tutti i membri del team.

E' utile prevedere la rotazione delle mansioni, al fine di limitare a specifici periodi l'esposizione allo stress che deriva dalla risposta diretta agli incidenti, oltre che aumentare il livello di sensibilità e di conoscenza di tutte le fasi operative su cui funziona il servizio. Sono inoltre da prevedere partecipazioni a conferenze e a corsi periodici sui temi rilevanti, sia per quelli tecnologici che per quelli più strettamente legali o di comunicazione istituzionale.

4) Tecnologia

Le tecnologie a supporto del CERT sono principalmente volte ad accumulare, valutare e condividere le informazioni in modo controllato, garantendo il supporto al processo di Incident Response anche in condizioni di emergenza. Quest'ultimo motivo spiega come mai i sistemi del CERT debbano essere necessariamente separati da quelli della Constituency, in modo tale da essere indipendenti e resilienti anche nel caso di perdita di disponibilità dei sistemi ICT che il CERT protegge.



L'essere separato ed indipendente dai sistemi ICT della Constituency talvolta viene visto come una perdita di efficienza, ma chi ha dovuto gestire incidenti di ampia portata può testimoniare come questa scelta, apparentemente diseconomica, sia stata fondamentale per ripristinare rapidamente i servizi della Constituency.

Il cuore del sistema informativo CERT è costituito dal Knowledge DB, che struttura in modo fruibile le informazioni trattate, siano esse "di contesto" (es. informazioni da Open o Closed Source Intelligence, dal SIEM del SOC, dal correlatore, dall'email) che specificamente legate ad un potenziale incidente (es. segnalazioni provenienti dal ticketing system). Il software di ticketing più utilizzato nei CERT di tutto il mondo è l'RTIR (Request Tracker for Incident Response).

5) Governo

La valutazione della bontà dell'azione del CERT si ottiene adottando alcuni classici strumenti di *Performance Management*. Uno degli errori tipici dei CERT immaturi è la mancanza delle informazioni necessarie per valutare il numero degli ingaggi e dell'efficacia delle procedure seguite per risolvere gli incidenti. Per ovviare a questo problema, è molto utile identificare fin dalla nascita del servizio quali possano essere gli indicatori da produrre verso la Constituency, che dimostrino il lavoro svolto e la capacità di indirizzare la chiusura efficace dell'incidente. Lo schema successivo riassume, ad alto livello, un approccio comune alla misurazione delle performance applicato al CERT.

	Obiettivo	Contenuto	
Policy Interne	▪ Fornire le procedure interne di funzionamento e le metriche del CERT e del modello Incident Response	▪ Assegnazione ruoli e responsabilità ▪ Descrizione del processo (servizio, organizzazione, tecnologia) ▪ Identificazione delle metriche chiave	COSA MISURO?
Indicatori	▪ Rappresentare in modo conciso le metriche sul CERT e sugli incidenti (KPI – Key Performance Indicator)	▪ Dalle metriche si identificano le fonti dati per realizzare la misura ▪ Tutte le fonti dati supportano il calcolo dei KPI per le componenti rilevanti del CERT	COME LO MISURO?
Cruscotto gestionale	▪ Interfaccia semplice e rapida per - informare il management - identificare le deviazioni dagli obiettivi	▪ Rappresentazione di tutti gli indicatori previsti, sia rispetto all'Incident Response che al funzionamento interno del CERT	COME LO RAPPRESENTO?

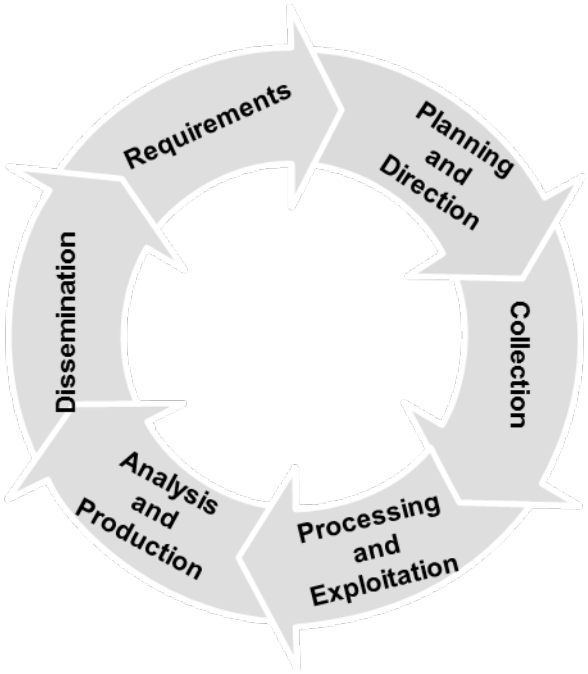
6) Abilitatori e strumenti

Per avviare il CERT ed aumentarne l'efficacia sono stati identificati sei abilitatori fondamentali che servono a identificare e gestire in modo strutturato, ripetibile e misurabile le informazioni relative agli incidenti.

Threat Intelligence

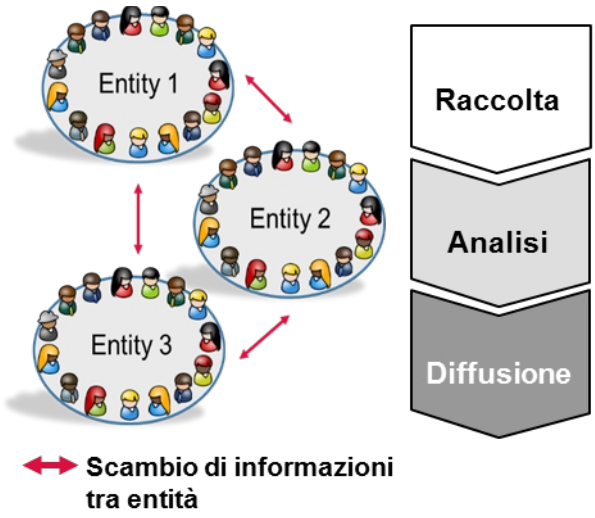
La "Threat Intelligence" è una capability essenziale per fare maturare la prevenzione e la gestione degli incidenti nella Constituency

L'obiettivo è integrare le fonti informative presenti nella fase di rilevazione con la conoscenza contestuale della Constituency e delle correlazioni (automatiche o manuali) all'interno del team di Analisti. Questa fusione di dati permette, tramite l'intelligenza e l'esperienza accumulata dal personale del CERT, l'individuazione dei "segnali deboli" di attacchi imminenti alle componenti più deboli o più sensibili della Constituency. Lo schema rappresenta il metodo standard adottato presso l'FBI per l'esecuzione delle attività di *Intelligence.*



Information Sharing

La condivisione delle informazioni è il cardine su cui si basa la corretta operatività del CERT. Questo processo deve potere seguire correttamente tutte le informazioni in ingresso, in elaborazione e in uscita dal CERT, mantenendo il corretto livello di classificazione e gestendo gli eventuali cambi di stato, sia in termini di riservatezza che di rapidità nella trasmissione. Per ottenere questo risultato è fondamentale riferire ad una chiara mappa degli interlocutori e ad una policy di classificazione e trasmissione codificata e condivisa, sia internamente che verso le entità a cui ci si rivolge


Entity 1
Entity 2
Entity 3
Raccolta
Analisi
Diffusione
Scambio di informazioni tra entità

Modello di Comando e Controllo

La comunicazioni con le altre entità deve essere affidabile e resiliente, soprattutto in caso di incidente. Per questo i diversi interlocutori devono essere raggiungibili tramite diversi canali di comunicazione, in modo tale che il mancato funzionamento di un canale non pregiudichi la continuità nella gestione dell'incidente. Questo requisito deve poter essere applicato ai diversi livelli della comunicazione, adottando per esempio due canali diversi per l'accesso alla rete da parte di due provider differenti, l'adozione di fonia fissa e mobile attestate a centrali ubicate in posizioni distanti l'una dall'altra, l'adozione di strumenti alternativi a quelli tradizionali (es. Canali radio o CB per comunicazioni voce, uso di Social Network per la diffusione di bollettini, linee telefoniche dedicate, …)

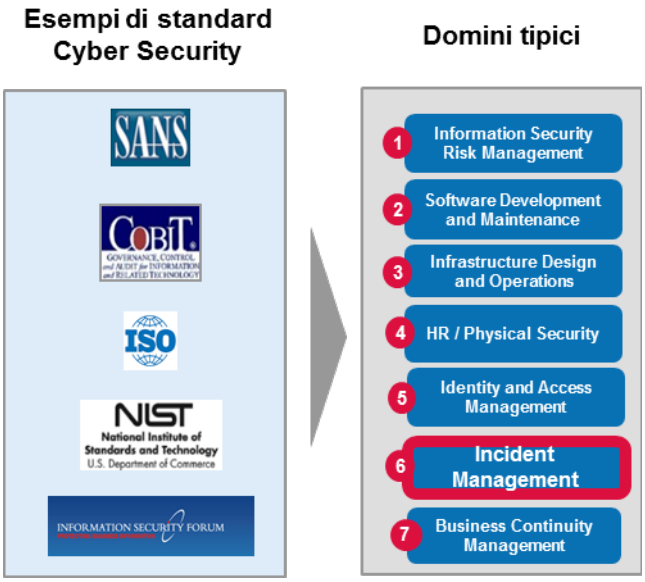
Affiliazioni / Certificazioni

L'accesso alle informazioni più preziose è subordinato al legame di fiducia con gli interlocutori con cui si opera. Le affiliazioni alle comunità CERT sono, di fatto, obbligatorie per la rilevazione e la gestione degli incidenti in modo efficace. Per aderire a queste associazioni serve un percorso di avvicinamento che permetta al CERT di essere conosciuto e riconosciuto all'interno della comunità. Per le due affiliazioni più importanti (e più difficili), che sono la FIRST e la TI, è fondamentale essere invitati da due sponsor: Una delle attività più impegantive per il responsabile e per il personale del CERT durante i primi due anni di attività del servizio è costituita dalla partecipazione a convegni e corsi, strumentali per incontrare e creare un forte legame con i rappresentanti degli altri CERT.

Agency	Target Recognition Level
enisa	Inclusion in ENISA CERT Inventory
FIRST	Full-Member Affiliation
TI	Trusted Introducer Accreditation
AUTHORIZED TO USE CERT	"Authorized to use CERT" endorsement

Standard

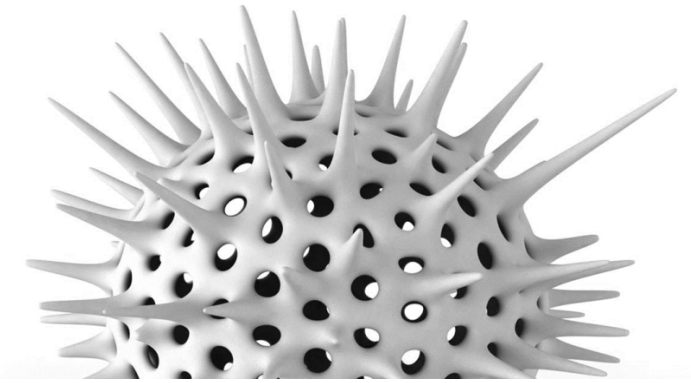
Riferire a standard riconosciuti globalmente facilita l'adozione delle competenze e la credibilità del CERT: in questo modo diventa facile confrontarsi con le esperienze esterne e fruire di linee guida che supportino e confortino le scelte operative da intraprendere nella realizzazione ed esercizio della funzione di gestione emergenze. Tutti gli standard di sicurezza prevedono un capitolo o una serie di requisiti legati al tema alla gestione e alla risposta agli incidenti.



Esercitazioni

Il CERT deve partecipare a tutte le esercitazioni disponibili per allenare e rendere automatici i comportamenti del team: solo tramite questo strumento è possibile capire i tempi di risposta previsti nell'esecuzione del processo di Incident Response, identificando le possibili aree di miglioramento e testando i diversi strumenti di condivisione, comando e controllo delle informazioni.

Questi esercizi possono essere organizzati internamente o possono essere allineati alle esercitazioni congiunte con altri enti/aziende sia nazionali che internazionali.



La corsa contro il tempo della cyber security

David Gubiani

Check Point

Dal 13 al 15 maggio scorsi si è svolto a Chiavari un evento importante per Check Point e Fabaris, suo partner storico. Durante i lavori del Simposio, incentrato sul tema della Cyber Defense, è stato posto in evidenza l'importante ruolo che vendor di sicurezza e laboratori di ricerca rivestono al fine di mantenere costantemente aggiornate le capacità di risposta alle minacce. È stata inoltre un'occasione per mettere in luce i principali trend di sicurezza, le sfide attuali e future che le aziende devono affrontare, e gli strumenti da adottare, pena la compromissione dei propri asset aziendali e gravi perdite economiche.

Il trend attuale richiede grande preparazione e cospicui investimenti: una stima dell'Europol ha infatti messo in luce che il cyber crime causa ogni anno perdite di denaro pari a ben 290 miliardi di dollari a livello globale, un business più profittevole del traffico globale di marijuana, cocaina ed eroina.

L'ultimo Security Report di Check Point ha messo bene in evidenza la crescita di malware sempre più sofisticato, che punta in maniera sempre più precisa ai dati aziendali, che possono essere trasformati con una certa facilità in denaro. Sono infatti finiti i tempi degli attacchi dimostrativi o delle iniziative personali, condotte più per spirito di sfida che per altro. Dietro al cybercrime oggi ci sono spesso organizzazioni internazionali, anche strutturate in modo complesso, che operano allo scopo di avere un ritorno economico, che permette di raggiungere a volte una marginalità decisamente superiori rispetto a quanto non possa offrire un qualsiasi mercato regolare.

Non si tratta più di piccoli fenomeni sporadici, ma di una vera e propria industria globale che cresce senza sosta. Si tratta solo dell'ulteriore conferma che il crimine informatico si è trasformato da tempo in un business fruttuoso: "I dati sono stati a lungo un obiettivo principale per gli hacker, considerando informazioni finanziarie, proprietà intellettuale, informazioni aziendali interne e credenziali di autenticazione." ha spiegato David Gubiani, Technical Manager, Check Point Software Technologies Italia. "Ora più che mai esistono differenti modi per far sì che i dati cadano nelle mani sbagliate poiché i dispositivi mobili e le app della cosiddetta "shadow IT" aprono nuovi vettori di attacco e alimentano il

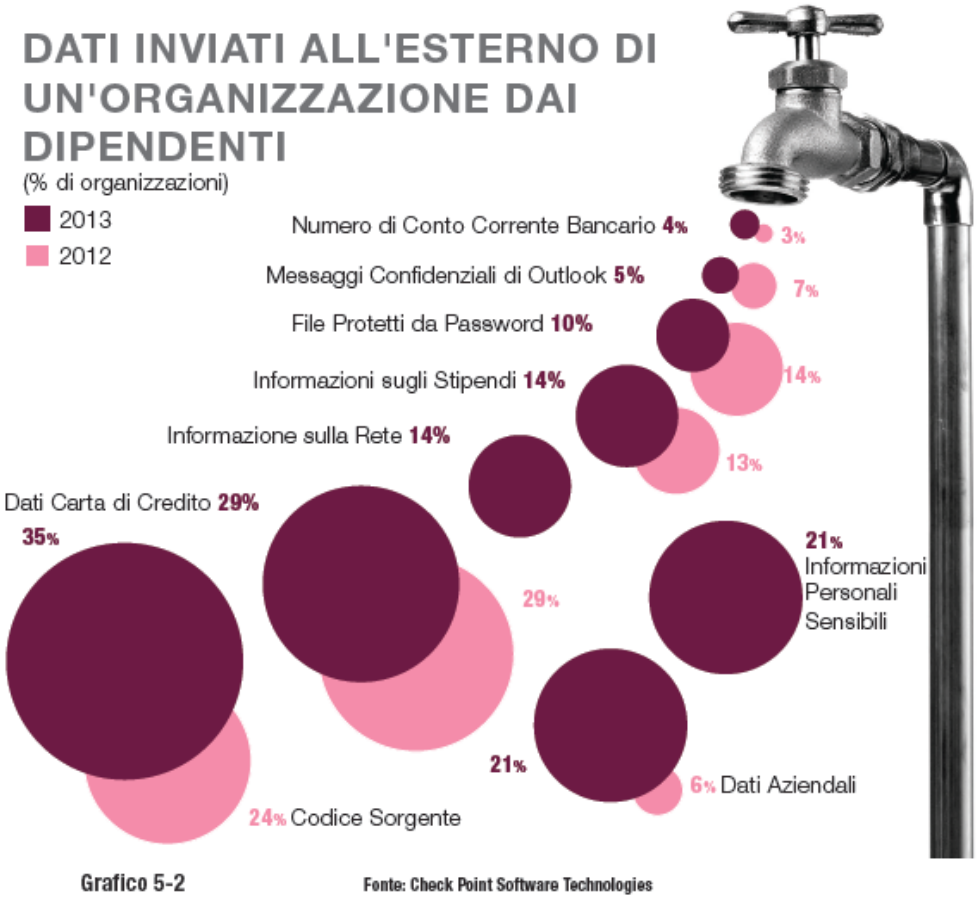
rischio di perdita o infiltrazione. L'Internet of Things aggrava ulteriormente la situazione dal momento che i dispositivi comunicano direttamente l'uno con l'altro per scambiare Informazioni su consumi di energia domestica, localizzazione e stato del proprio veicolo, tracciamento pacchi, salute personale e altro ancora." ha continuato. Poiché una maggiore quantità di dati viene traferita in modi differenti, diventa più difficile che mai controllarli e proteggerli.

Gli hacker non rappresentano l'unica minaccia per i dati aziendali. Molte violazioni accadono inavvertitamente, quando gli utenti inviano il file sbagliato al destinatario giusto, o il file giusto al destinatario sbagliato – o semplicemente lasciano un laptop non protetto nel posto sbagliato. L'errore umano ha giocato un ruolo chiave in molti degli incidenti di data loss degli anni passati ma, che si tratti di una cosa intenzionale o meno, il risultato può essere lo stesso: i dati sensibili sono esposti a rischi, clienti arrabbiati, reputazione danneggiata, multe dovute a mancanza di conformità e interruzioni critiche al business.

In particolare, la ricerca di Check Point ha rilevato che nel corso del 2013, ben l'88% delle aziende analizzate ha riscontrato almeno un evento di perdita di dati, il che significa che una parte di dati sensibili è stata inviata all'esterno dell'organizzazione via e-mail o caricata via web browser. Si tratta di un aumento drastico rispetto al dato già elevato di 54% osservato nel 2012, e mette in luce the la lotta costante delle organizzazioni per proteggere dati sensibili dall'esposizione accidentale o intenzionale. Sempre parlando di soldi, nel 33% delle istituzioni finanziarie intervistate, informazioni di carte di credito sono state inviate all'esterno delle organizzazioni stesse.

Ogni giorno, un'organizzazione riscontra 29 eventi di esposizione potenziale di dati sensibili, e ogni 49 minuti vengono inviati dati sensibili al di fuori di un'organizzazione. Questo è un tasso preoccupante per qualsiasi organizzazione in ogni settore, e sottolinea la necessità di controlli più aggressivi attorno ai dati sensibili.

Nello scenario odierno di crescenti perdite di dati, le organizzazioni devono agire per proteggere i dati sensibili. Il miglior modo di prevenire la perdita di dati non intenzionale è di implementare una policy aziendale automatica che rileva questi incidenti prima che i dati lascino l'organizzazione. Tali policy possono essere messe in atto al meglio attraverso una soluzione di Data Loss Prevention (DLP). I prodotti di DLP contentaware offrono una vasta gamma di funzionalità e presentano alle organizzazioni differenti opzioni di implementazione.



Il Simposio ha anche rappresentato un'occasione per mettere in luce alcune qualità della tecnologia Check Point, come ad esempio la gestione unificata della sicurezza IT, semplificata dalle "smart console", che migliorano la gestione della Sicurezza e offrono efficaci viste sintetiche al personale coinvolto nelle operazioni di Cyber Defense. Inoltre, è stata un'occasione per dare evidenza del valore che un system integrator può offrire nel diffondere nuovi modi per affrontare le moderne minacce informatiche. "Il mondo della Difesa, pur declinando con proprie peculiarità gli orientamenti dei player della Sicurezza Informatica, è oggi in grado di cogliere i vantaggi che un vendor specializzato come Check Point può offrire e mantenere nel tempo" – ha dichiarato Emanuele Madeo, Direttore della Business Unit ICT & Security di Fabaris, che ha aggiunto: "I nostri risultati sono la felice conseguenza di un programma di aggiornamento costante e delle numerose esperienze maturate al fianco del nostro partner."

Fabaris, dopo la recente acquisizione della certificazione ISO 27001, pone al centro della propria azione una tecnologia eccellente e un modello ispirato alle migliori prassi, al fine di dare un concreto sostegno all'Amministrazione. "Il contributo che l'Industria può dare per garantire flessibilità e standard qualitativi elevati è di notevole spessore e richiede ingenti sforzi" – ha continuato Madeo, descrivendo i passi compiuti in risposta alle esigenze della clientela. Infatti, Fabaris, Gold Partner Check Point, aderendo al programma CCSE (Certified Collaborative Support Partner) mette a disposizione le proprie migliori risorse per fornire supporto di elevato livello ai clienti di livello "large enterprise".

“Fortunatamente esistono contromisure efficaci. Check Point dispone di strumenti che in meno di un’ora sono in grado di creare report completi che identificano lo stato di protezione, i rischi attivi e le problematiche di sicurezza di un’organizzazione, assieme alle attività sospette e possibili perdite e fughe di dati, fornendo raccomandazioni mirate su come risolvere in maniera specifica tali rischi e ottenere una sicurezza completa,” ha concluso Gubiani.

Organizzazione, metodo e tecnologia: le armi per la cyber defence

Antonio Papa e Marco Dattrino

EPS Datacom

Gli scorsi 14 e 15 maggio, nella suggestiva ambientazione dell'Auditorium di Chiavari - ricavato all'interno della chiesa di San Francesco, risalente al XIII secolo - si è svolta la terza edizione del ***Cyber Defence Symposium*** organizzato dalla Scuola Telecomunicazioni delle Forze Armate di Chiavari con la partecipazione di esponenti della sicurezza provenienti da diverse realtà, compresi rappresentanti delle Istituzioni, delle Forze Armate, delle Forze di Polizia, di aziende specializzate ed di enti di ricerca.

La scuola è stata iniziatrice di un percorso sul tema della *Cyber Defence* e *Information Security*, tema su cui, fortunatamente, esiste una sempre maggiore consapevolezza da parte delle istituzioni civili e governative. In particolare, la scuola sta diventando il fulcro per la fondamentale azione di alfabetizzazione ed educazione relativa alla sicurezza informatica rivolta alla formazione delle nuove figure professionali della Pubblica Amministrazione, come dichiarato dall'allora direttore dell'Agenzia Italiana per il Digitale, Ing. Agostino Ragosa.

In questo articolo si vuole richiamare l'attenzione sull'intervento congiunto dell'Ing. Antonio Papa, della EPS Datacom Srl e del Dott. Marco Dattrino, Security Business Analyst CSI Piemonte. L'ing. Papa ha affrontato il tema del corretto approccio alla *Cyber Defence* che dovrebbe essere parte integrante delle attività operative di tutte le organizzazioni e che, invece, presenta ancora ampi spazi di miglioramento – soprattutto a livello di consapevolezza del top management. Il dott. Dattrino ha portato l'esperienza del CSI Piemonte che recentemente ha gestito, con danni molto limitati, un pesante attacco DDOS e che, grazie alle analisi a posteriori sull'attacco e al successivo affinamento dell'architettura di difesa, è stato in grado di subire un attacco cinque volte più intenso – in termini di dimensioni e durata – senza danni.

Il generale Keith Alexander, Head of NSA and *US Cyber Command* fino allo scorso 28 marzo, ha dichiarato che " i furti compiuti con mezzi informatici a danno delle reti di organizzazioni pubbliche e private, incluse le aziende di Fortune 500, rappresentano **il più grande trasferimento di ricchezza nella storia umana**" e sul sito dell'FBI si specifica che non si tratta del semplice furto di danaro, ma di derubare le persone delle loro idee, invenzioni ed espressioni creative, ciò che viene usualmente indicato come proprietà intellettuale.

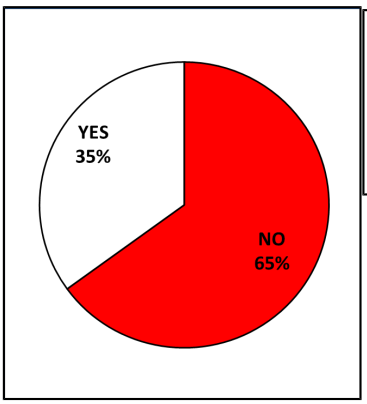
E si quantifica il danno per il sistema economico americano in miliardi di dollari oltre la distruzione di migliaia di posti di lavoro. E, oltre l'NSA e l'FBI, l'allarme è sollevato da tutti gli altri enti governativi USA – solo per parlare di un paese usualmente preso a riferimento - compresa la Casa Bianca, il Congresso, la SEC, il DHS.

In parallelo il perimetro di attacco è in continua espansione grazie ai nuovi modelli organizzativi che fanno della digitalizzazione e della mobilità gli elementi portanti, con il risultato di moltiplicare esponenzialmente le vulnerabilità e gli spazi da difendere.

Nonostante l'altissimo livello di allarme generato da molteplici – e una volta impensate – fonti e a fronte della sempre maggiore vulnerabilità delle organizzazioni, ci si aspetterebbe che nelle organizzazioni private

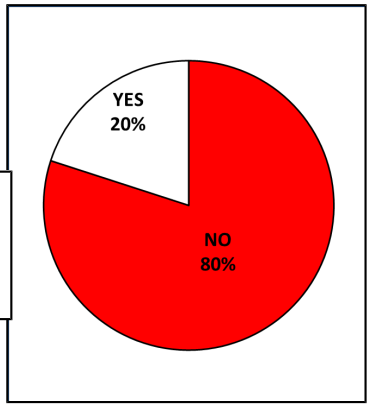
e pubbliche la gestione della minaccia Cyber fosse una attività regolarmente inclusa nei processi interni di risk management, ma non è così.

Una recente ricerca della PwC (PricewaterhouseCoopers), che ha intervistato 1300 CeO a livello mondiale, ha evidenziato un'allarmante mancanza di consapevolezza del top management se ben due Amministratori Delegati su tre non sono preoccupati della perdita dei dati dei loro clienti o della perdita di asset aziendali coperti da proprietà intellettuale e solo il 20% ritiene realistica la possibilità di un attacco informatico alla propria azienda quando chiunque operi nel settore sa bene che la domanda da farsi non è "quante probabilità ho di essere attaccato?" quanto piuttosto "quando mi hanno bucato?"



E' preoccupato della perdita di asset aziendali protetti da proprietà intellettuale o di dati dei suoi clienti?

Ritiene realistica la possibilità di un attacco informatico alla sua azienda?



F*PwC* A conferma di questi dati preoccupanti arriva un altro report – questo a livello USA – il *PwC 2013 US State of Cybercrime Survey* che ha visto intervistati oltre 500 esperti e responsabili, in ambito sicurezza, di organizzazioni private e governative USA. Tale rapporto ha verificato che solo il 40% delle organizzazioni hanno implementato una metodologia che consenta di verificare l'efficacia dei programmi di sicurezza, in mancanza della quale i piani– anche quando esistono - perdono completamente di significato.

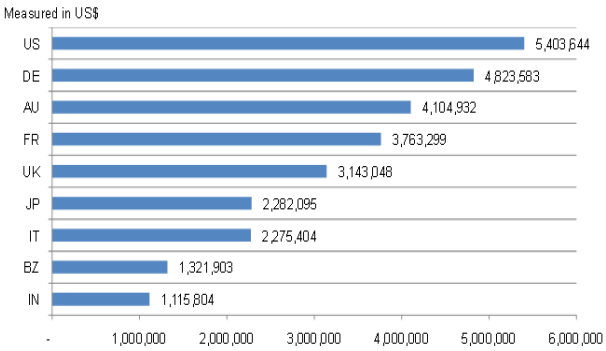
Lo stesso rapporto definisce il top management di queste numerosissime organizzazioni come le classiche "*frog in the pot of hot water"* con riferimento all'esperimento pseudo-scientifico – molto noto nei paesi anglosassoni – secondo il quale una rana messa in una pentola di acqua bollente salta immediatamente fuori, mentre se l'acqua è tiepida e viene riscaldata molto lentamente la rana si rilassa e non ne esce viva, perché il suo sistema di allarme non è programmato per quel tipo di minaccia.

Analogamente il rischio corso dalle organizzazioni non consapevoli è quello di accorgersi del problema quando il danno è compiuto e, nel caso delle aziende, la sopravvivenza stessa è messa in discussione. Ci sono innumerevoli casi in cui la sottrazione di prodotti – tipicamente SW - ma non esclusivamente – costati anni di lavoro e investimenti può essere immesso sul mercato da concorrenti sleali a prezzi stracciati che sono comunque remunerativi considerata l'assenza di costi di sviluppo.

Un noto esempio è il caso della American Superconductor Corp (AMSC), azienda specializzata in sistemi di controllo per turbine eoliche. Questa società, con sede nel Massachusetts, ha scoperto che il suo prodotto più importante era stato clonato a favore del suo più grande cliente, la cinese Sinovel che vende e gestisce turbine eoliche in tutto il mondo. Fino al marzo 2011, Sinovel ha acquistato il prodotti e servizi da AMSC

per oltre 100M USD e aveva un contratto firmato per ulteriori 700M USD. Nel marzo 2011, senza alcun preavviso, Sinovel interrompe gli acquisti generando un danno economico da cui l'azienda non si è più ripresa (in figura il grafico del valore dell'azione con il crollo concomitante alla cancellazione degli ordini da parte del cliente cinese).

La protezione delle informazioni e dei dati riservati sarà un elemento strategico per aziende e organizzazioni, ma anche i costi diretti stanno diventando sempre più rilevanti come certificato dallo studio del Ponemon Institute "*Cost of Data Breach Study: 2013 Global Analysis*" che ha analizzato 277 incidenti verificandone, in dettaglio, l'impatto sui costi diretti (figura).



Il risultato evidenzia un costo medio per incidente che va dal milione di euro per l'India a oltre cinque milioni per gli USA. Inoltre i costi sono proporzionali alle dimensioni dei *data breach* e sono destinati a crescere costantemente in funzione del continuo, inevitabile, trasferimento e mantenimento in forma digitale di dati sensibili.

La buona notizia è che un'altissima percentuale degli attacchi può essere gestita internamente dalle organizzazioni aumentando il proprio livello di resilienza attraverso la definizione di una organica strategia, necessariamente dinamica, per la Cyber Security.

Tale strategia si deve fondare su almeno cinque elementi, il primo dei quali è sicuramente lo sviluppo di una ***Cyber Security Education***: ad oggi, i danni più elevati alle organizzazioni non derivano da attacchi malevoli esterni – almeno non direttamente – ma da attacchi dall'interno, consapevoli e inconsapevoli.

Una corretta informazione è senza dubbio l'investimento con il più alto rapporto benefici/costi in termini di protezione delle informazioni e il programma deve coprire tutto l'ecosistema della organizzazione, inclusi fornitori e consulenti che spesso risultano essere l'anello debole della catena di difesa.

Il secondo elemento è sicuramente la **tecnologia**, che per complessità sempre maggiore e velocità di evoluzione – assolutamente necessaria per tentare di rimanere ad un livello adeguato alla minaccia – deve essere però correttamente inserita, da specialisti, in una architettura difensiva che deve tenere in considerazione tutti i possibili elementi di vulnerabilità del sistema.

Il terzo elemento è il controllo, il **monitoraggio** e il *tuning* della tecnologia che se non viene costantemente verificata a confronto della rapidissima evoluzione della minaccia rende vani anche gli ingenti investimenti effettuati sulla tecnologia stessa.

Questi primi tre elementi riescono ad abbattere l'80% degli attacchi mediamente portati a tutte le organizzazioni. Per una protezione che arrivi fino al 95% degli attacchi è necessario espandere la strategia completando gli elementi precedentemente menzionati con una *Situational Awareness* fondata su due pilastri: una ***Asset Identification*** che definisca gli asset strategici per l'organizzazione indicando chiaramente gli obiettivi sensibili e focalizzando la strategia difensiva sugli stessi ed una ***Threat Awareness***, che si traduce nella ricerca delle potenziali minacce presenti nell'ecosistema spostando la prima linea difensiva al di fuori dell'organizzazione da difendere.

Resta scoperto un 5% di casi che ricadono nell'ambito di attacchi estremamente sofisticati e mirati, come gli *state sponsored attack* che richiedono la cooperazione con organismi di difesa a livello governativo.

L'intervento dell'ing. Papa è stato integrato e completato dall'intervento del dott. Dattrino che ha condiviso l'esperienza di un recente attacco subito dal CSI Piemonte e di come un approccio integrato, coerente con quanto esposto precedentemente, e l'analisi post-attacco siano stati elementi chiave nel mitigare l'impatto dell'attacco stesso e a fornire le informazioni necessarie a fare il *tuning* delle difese che hanno successivamente retto ad un attacco molto più violento senza danno alcuno.

Il dott. Dattrino ha introdotto, al fine di comprendere meglio quanto accaduto, ruolo e dimensioni del CSI Piemonte che risulta essere la principale azienda italiana pubblica del settore ICT e che eroga servizi in ambito sanità, attività produttive, beni culturali e sistemi amministrativi. Tra le altre attività IL CSI è incaricato del full outsourcing della Regione Piemonte, del Consiglio Regionale, della Provincia e della città di Torino, oltre a più di 110 enti consorziati che usufruiscono dei servizi del datacenter. Gestisce servizi di telecomunicazioni e integra il tutto con servizi di security.

Il 25 Ottobre 2013 un attacco Ddos, rivendicato da Anonymous, ha colpito l'infrastruttura del CSI Piemonte comportando un drastico aumento dei tempi di accesso ai siti istituzionali. La portata dell'attacco è stato di 4 Gb ed è durato 4 ore. I sistemi designati a proteggere la rete dagli attacchi DDOS sono stati piuttosto efficaci consentendo un ripristino completo delle funzionalità in poche ore, ma una analisi dettagliata, completata anche da attività di *data mining* incluso il confronto fra *log analysis* e eventi sui *social network*, quello fra volumi, origine e andamento del traffico di rete, ha consentito una revisione ed un affinamento delle contromisure a miglioramento del sistema di protezione. L'ottimizzazione dei sistemi di prevenzione e l'efficacia del lavoro di analisi post-attacco è risultato evidente a seguito di un successivo attacco DDOS di entità molto maggiore rispetto a quello del 25 ottobre che è stato assorbito senza disservizi.

In conclusione, sono evidenti i segni del crescente livello di diffusione, aggressività e sofisticazione della minaccia informatica cavalcata da diversi attori: gruppi criminali sempre più organizzati, efficienti e sovranazionali, gruppi di Hacktivist sempre più strutturati ed organizzazioni governative più o meno ufficiali.

In positivo si conferma che, a fronte di una adeguata consapevolezza e sostegno da parte del top management, è possibile contenere la maggior parte degli attacchi e mitigarne gli effetti a condizione di implementare una strategia di difesa dinamica che tenga conto di tutti gli elementi chiave: il fattore umano, la scelta delle tecnologie e il loro monitoraggio, l'identificazione degli asset strategici da proteggere e la continua esplorazione dell'ecosistema da cui proviene la minaccia.

Cisco Cyber Security

Un approccio architetturale per la realizzazione della “Internet of Everything”

Fabrizio Gergely

Cisco

Executive Summary

Cisco è protagonista da oltre vent'anni dell'evoluzione delle Reti e da sempre ha anticipato le transizioni del mercato, sviluppando architetture e soluzioni innovative che sono alla base di Internet. Ora che nuove persone, processi, dati, cose possono connettersi e interagire grazie alla Rete, accade qualcosa di straordinario: l'**Internet of Everything** (IoE) ha un impatto paragonabile a una "nuova rivoluzione industriale" in quanto permette di esaltare, grazie all'evoluzione tecnologica, elementi che caratterizzano storicamente il nostro tessuto industriale e la nostra società, creatività, talento innovativo, qualità, capacità di produrre eccellenza in ogni campo.

Cisco si pone quindi legittimamente alla guida del percorso verso l'Internet of Everything. Comprendere fin dall'inizio la portata di questa rivoluzione è essenziale per le aziende e per il Paese al fine di creare sviluppo, trasformazione e innovazione. Internet of Everything, infatti, si pone l'obiettivo di cambiare radicalmente il modo di fare impresa, di imparare, di essere cittadini.

Componente fondamentale per abilitare questa trasformazione è la **CyberSecurity** che deve essere applicata in ogni contesto o soluzione informatica per fare fronte alle odierne minacce che rendono necessario un approccio olistico, architetturale ed innovativo.

Analizziamo di seguito tre aspetti rilevanti in ambito CyberSecurity:

- Le piattaforme tecnologiche
- La formazione
- I processi

Le Piattaforme tecnologiche

AntiSec, LulzSec, Anonymous. Violazioni della sicurezza di alto profilo che hanno interessato un elenco infinito di giganti commerciali e di produttori di beni di consumo. Secondo alcuni osservatori le tecnologie esistenti per la sicurezza di reti e computer sono inadeguate per il compito cui sono preposte. Sono progettate per un mondo molto diverso, un mondo composto da sistemi statici e da procedure chiaramente articolate e applicate per il cambiamento, un mondo dove le reti sono circondate da perimetri ben definiti e difendibili.

Consideriamo invece il mondo reale, nel quale i responsabili della sicurezza effettivamente operano:

- Aumento esponenziale della velocità di mutamento. Virtualizzazione, mobilizzazione e consumerizzazione dell'IT fanno muovere ed evolvere rapidamente i bersagli degli attacchi, complicandone la protezione.
- Maggiore connettività. I collegamenti con partner e clienti e la disponibilità "infinita" e

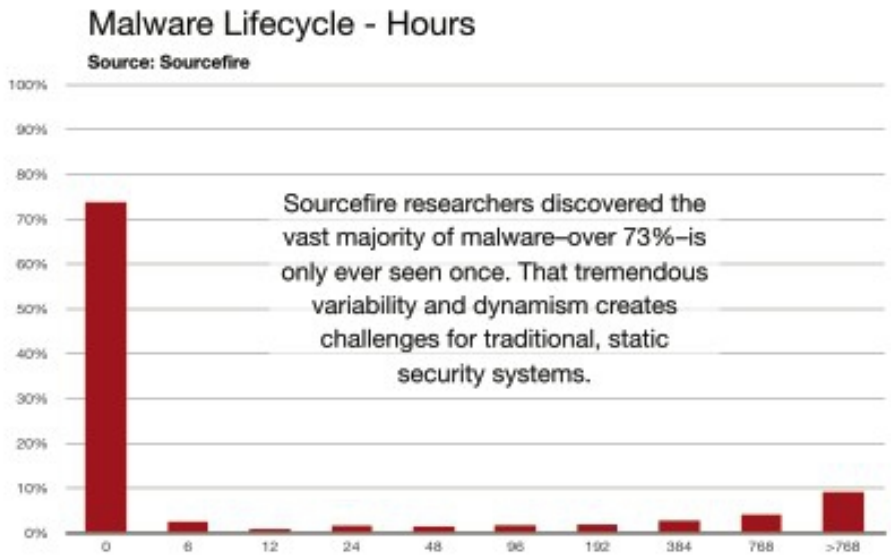
crescente di applicazioni, dispositivi e sistemi facilitano l'accesso alle risorse sensibili.

- Aggressori sempre più sofisticati. Il crimine organizzato e le nazioni ostili producono aggressori motivati, ben addestrati e con cospicue disponibilità finanziarie.

Gli odierni strumenti della sicurezza erano stati progettati per un ambiente stabile, che mutava lentamente. Tali strumenti presupponevano che i responsabili IT e della sicurezza avessero il tempo di prevedere gli attacchi e di prepararsi adeguatamente per bloccarli tutti. Ora, nell'attuale ambiente informatico dinamico, questi strumenti statici si sono rapidamente rivelati inefficaci. I problemi di fondo sono due:

- La mutazione dell'ambiente. I cambiamenti rapidi che hanno interessato risorse, utenti, applicazioni e sistemi hanno causato la perdita di contatto tra gli strumenti di sicurezza e l'ambiente che dovrebbero difendere. In più, le reti estese che includono endpoint, dispositivi mobili, computer virtuali e centri dati implicano un maggior numero di risorse da proteggere.

- La mutazione degli attacchi. L'industrializzazione della pirateria informatica ha portato attacchi più complessi, in grado di eludere anche le difese multilivello. Il ciclo di vita delle minacce si misura adesso in ore, per questo le difese di tipo statico risultano sempre più inadeguate.



Cisco con la recente acquisizione di Sourcefire, la più rilevante acquisizione in termini valore ad oggi operata nel campo della Security, propone al mercato una visione che riflette la realtà delle odierne discipline per la sicurezza di reti e computer.

L'innovazione consiste in un'architettura che fornisce una protezione efficace perchè consiste in un processo continuo che affronta l'intero continuum dell'attacco con quattro elementi essenziali:

- **Visione**. Chiarezza e visione che riflettono la realtà dell'ambiente come è in questo momento
- **Apprendimento**. Applicazione delle informazioni ai dati grezzi per migliorare la comprensione e il processo decisionale.
- **Adattamento**. Evoluzione e modifica automatiche delle difese in risposta ai cambiamenti.
- **Azione**. Reazioni decisive, flessibili e automatizzate agli eventi.

Visione

L'agilità richiede chiarezza, ma troppo spesso la sicurezza tradizionale è cieca al mutamento delle condizioni e ai nuovi attacchi. Questa mancanza di approfondimento limita la capacità di analisti, amministratori e responsabili di valutare gli eventi e pertanto ne riduce le opzioni di reazione. Le soluzioni Cisco Sourcefire danno accesso immediato a informazioni di ampiezza e profondità senza precedenti, supportando la visibilità di:

- **Mappa della rete**. Viene realizzato un profilo esaustivo e completo dei dispositivi connessi

alla rete, compresi telefoni cellulari, stampanti, computer, virtual machines e molte altre risorse.

- **Attacchi alla rete e malware**. Dati dettagliati sui singoli attacchi e sulle tendenze generali che attraversano la rete fino agli endpoint.
- **Sistemi operativi**. Vengono incluse informazioni specifiche sulla versione e sulle vulnerabilità note, approfondendo i
rischi potenziali e le problematiche della sicurezza.
- **Applicazioni, servizi e protocolli**. Vengono evidenziate le app non autorizzate e i servizi non protetti o non necessari, che sono vettori di attacco comprovati.
- **Identità** . Comprensione esatta di chi si trova nella rete, di cosa fa e della sua posizione.
- **Comportamento della rete**. Individuazione delle alterazioni e delle modifiche a configurazioni, connessioni e al flusso delle informazioni, che sono un indicatore attendibile della riuscita compromissione del sistema.

Altro elemento importante in aggiunta all'ampiezza della visione, è la profondità dei dati forniti da Cisco Sourcefire. Per esempio, gli analisti possono passare rapidamente dall'esame di tendenze e allarmi ad alto livello all'analisi dettagliata dei singoli pacchetti inviati dalla sessione di un aggressore. I responsabili hanno un accesso immediato al preciso livello di visibilità necessario per affrontare qualsiasi dubbio o situazione.

Apprendimento

La visibilità genera dati. Per poter prendere decisioni efficaci in risposta a quei dati è necessario un apprendimento rapido. L'apprendimento richiede una continua analisi delle informazioni, generate sia a livello locale che collettivamente dalla comunità, al fine di ottenere una prospettiva. Cisco Sourcefire correla gli eventi con le conoscenze, come metodo essenziale per capire e per prendere decisioni; le reazioni sono pertanto ordinate per priorità, automatizzate ed informate.
Per esempio, l'applicazione delle informazioni fornisce un mezzo per capire quali attacchi richiedono una reazione oppure ulteriori indagini. E se c'è un tentativo di sfruttare una vulnerabilità di una specifica versione del sistema operative Windows? Se il bersaglio dell'attacco usa la versione vulnerabile del sistema, ci sono buone probabilità che sia stato compromesso.
Invece i tradizionali sistemi di sicurezza non conoscono il bersaglio, quindi non hanno modo di valutare la rilevanza di un attacco. Tutti gli allarmi diventano essenzialmente uguali e devono essere valutati manualmente.

Le soluzioni Cisco Sourcefire offrono le informazioni necessarie per valutare tali attacchi, per esempio rilevando quale sistema operativo è in uso nel bersaglio, determinando quali sono gli eventi significativi e riducendo drasticamente il numero di eventi fruibili, fino al 99%. Con un'infrastruttura che può continuamente raccogliere e analizzare i dati per creare le
informazioni di sicurezza è inoltre possibile, tramite l'automazione, identificare gli indicatori della violazione, rilevare malware sofisticati in grado di alterare il proprio comportamento per evitare il rilevamento, quindi eseguire un'azione correttiva. Le violazioni che sarebbero passate inosservate per settimane o mesi possono essere ora identificate, valutate, contenute e rimosse rapidamente. Le funzioni di apprendimento di Cisco Sourcefire possono essere ulteriormente ampliate tramite l'integrazione con altri sistemi di sicurezza, come quelli di gestione delle vulnerabilità. Le soluzioni Cisco Sourcefire ampliano il proprio database delle vulnerabilità con informazioni aggiornate che consentono precisione e accuratezza.

Le soluzioni Advanced Malware Protection di Cisco Sourcefire illustrano ulteriormente la potenza dell'apprendimento grazie a Collective ImmunityTM. Le informazioni riguardanti le attività illecite osservate in un sistema, in qualunque parte del mondo, possono essere immediatamente condivise con tutti gli altri utenti. I sistemi ottengono automaticamente protezione dai nuovi attacchi. Questi dati fungono anche da "scatola nera" per la sicurezza, migliorando la protezione intelligente e il processo decisionale.

Adattamento

Le reti cambiano, i bersagli cambiano, gli attacchi ed anche le motivazioni di un aggressore cambiano.
E come reagisce la maggior parte delle soluzioni di sicurezza a tale dinamismo? Senza cambiare. O comunque non cambiano senza uno sforzo considerevole e ad un ritmo che lascia le risorse aperte ad essere sfruttate.
Le nuove minacce richiedono delle nuove regole di rilevamento, o firme. Le nuove policy organizzative richiedono ai singoli di modificare le impostazioni esistenti.
E se nuove risorse o sistemi compaiono nella rete? La maggior parte dei sistemi di sicurezza in uso neanche se ne accorgerà,
men che meno reagirà.
I comportamenti nella rete, come le connessioni e le sessioni inattese, segno importante di una possibile violazione, passano inosservati. Dato che il ciclo di vita delle minacce viene correntemente misurato in ore, gli approcci attuali lasciano i sistemi vulnerabili ed esposti. Le soluzioni Cisco Sourcefire forniscono funzioni essenziali che consentono ai sistemi di sicurezza di adattarsi ed evolversi automaticamente in reazione ai cambiamenti:

- L'ottimizzazione della difesa regola automaticamente le policy di sicurezza per mantenere il passo con i cambiamenti di ambienti specifici.
- L'applicazione del rispetto delle policy supporta la capacità di bloccare endpoint e reti per prevenire le modifiche
non autorizzate e ridurre la superficie di attacco disponibile.
- Un'architettura aperta supporta personalizzazione e modifica complete delle funzioni di rilevamento.

- Soluzioni di sicurezza universali, flessibili, che consentono la rapida distribuzione esattamente del tipo di protezione necessaria, proprio dove serve.

Azione

La responsabilità essenziale di qualsiasi sistema di sicurezza è quella di proteggere risorse e dati. Gli attacchi devono essere bloccati. Le policy, applicazioni consentite, dispositivi supportati, attività proibite, devono essere applicate. Gli eventi sospetti devono essere ordinati per priorità e comunicati agli analisti. Le infezioni di malware devono essere controllate per minimizzare i danni. Cisco Sourcefire offre quattro funzioni essenziali per agire in modo rapido, decisivo ed efficiente:

- **Flessibilità**. Le risposte agli eventi di sicurezza possono variare in modo illimitato. Le funzioni di definizione, gestione ed applicazione di policy esaustive assicurano una reazione adeguata.
- **Assegnazione delle priorità**. Le soluzioni Cisco Sourcefire dispongono di funzioni esclusive per la valutazione e per l'assegnazione delle priorità alle minacce. Il rumore di fondo viene eliminato, consentendo ai responsabili di concentrarsi sulle minacce più importanti.
- **Velocità**. Le appliance ad alte prestazioni, specificamente progettate, valutano le attività alla velocità del trasferimento dati. Gli aggiornamenti all'infrastruttura in tempo reale sono rilevati e valutati dalla tecnologia Cisco Sourcefire per l'automazione di sicurezza e consapevolezza.
- **Sicurezza retroattiva**. Cisco Sourcefire ha la capacità di identificare, esaminare, tracciare, indagare e rimuovere il malware, anche quando nella rete penetrano dei file malevoli originalmente classificati come "sicuri" o "sconosciuti".

L'integrazione con altri strumenti di sicurezza e di gestione di sistemi e reti amplia la capacità di azione delle soluzioni Cisco Sourcefire. Questi collegamenti rendono possibile condividere dati e azioni tra i sistemi, applicando le informazioni per reagire in modo più rapido e pertinente agli eventi. Il programma Technology Partner di Cisco Sourcefire mette a disposizione integrazioni supportate e testate con un mix diversificato di tecnologie di rete e di gestione, fra le quali:

- **Gestione delle informazioni e degli eventi di sicurezza**. Semplice condivisione delle informazioni sulle intrusioni grazie alle piattaforme SIM/SEM.
- **Gestione di sistemi e reti**. Sistemi di gestione potenziata delle operazioni con i dati di sicurezza rilevanti.
- **Analisi forense**. Fornisce in tempo reale informazioni sulle risorse e sugli attacchi agli strumenti di analisi forense.
- **Controllo dell'accesso alla rete**. Messa in quarantena dei sistemi sospetti e applicazione della

conformità alle policy tramite l'integrazione con le tecnologie di accesso alla rete.

- **Sicurezza delle applicazioni**. Protezione delle applicazioni basate sul web contro le vulnerabilità note e le "falle" nella sicurezza.

La Formazione

Dal punto di vista delle Persone, l'informazione e la formazione sono due elementi imprescindibili per riuscire a permeare un'organizzazione delle competenze di sicurezza necessarie per gestire la complessità dell'attuale scenario.

Il numero di persone e, soprattutto, di aziende che si affacciano al networking, sia con reti locali che geografiche ed alla sicurezza, continua a crescere vertiginosamente, ma le risorse umane qualificate per la progettazione, la realizzazione, l'implementazione e la manutenzione di una rete diventano sempre più esigue: problema che tocca da vicino sia i fornitori di tecnologia, sia le aziende che hanno sempre maggiori difficoltà a reperire personale, interno ed esterno, in grado di rispondere alle problematiche legate alle più recenti tecnologie di networking, sicurezza e comunicazione elettronica.

È proprio per colmare questo divario che Cisco, leader mondiale del networking per Internet, ha messo a punto **Cisco Networking Academy Program**, un programma completo di formazione che consente di imparare ad operare su reti di piccole, medie e grandi dimensioni.

Il programma si rivolge ad organizzazioni no--profit, siano esse Università, istituti superiori, enti pubblici, centri di formazione professionale. Ad oggi, sono state istituite nel mondo più di **10.000** Networking Academy e sono oltre **1 milione** gli studenti che frequentano corsi in **165** Paesi. In **Italia**, operano più di **300** Networking Academy: Centri di Formazione, Istituti scolastici, Università e Amministrazioni Pubbliche che, aderendo al Programma, hanno qualificato oltre 600 docenti e che ogni anno attivano classi per oltre 20.000 studenti.

Il Programma Cisco Networking Academy, studiato da esperti della formazione, viene erogato in modalità blended coniugando auto--apprendimento in modalità eLearning, formazione in aula attraverso tutor ed esercitazioni pratiche in laboratorio: un modello di riferimento che ottimizza l'efficacia dell'apprendimento.

Sottolineando il suo impegno per l'eccellenza nel campo dell'istruzione e certificazioni, Cisco ha recentemente annunciato che il corso **CCNA Security** è stato approvato come certificazione ufficiale da parte del Dipartimento della Difesa Americano (DoD) 8570,01--M.

La direttiva DoD 8570 fornisce le linee guida e le procedure per la formazione, la certificazione e la gestione di tutti i dipendenti del Dipartimento della Difesa che svolgono funzioni di Information Assurance nei loro compiti assegnati. Questi individui sono tenuti a svolgere un percorso di formazione e delle certificazioni per il loro ruolo e per la classificazione delle informazioni gestite.

La certificazione CCNA Security è stata approvata per i livelli di informazione DoD Assurance Tecnico I e II. Cisco Systems è il primo vendor ad offrire un robusto portafoglio di certificazioni di rete che soddisfa lo standard ISO 17024 accreditato da ANSI.

In italia operano diverse Network Academy create e gestite dall'Amministrazione della Difesa che garantiscono, su diverse Forze Armate e sedi, formazione annua specialistica su tecnologie di networking a centinaia di Persone dell'Amministrazione con il vantaggio per la stessa di poter avere un Potenziale umano di Professionisti aggiornati allo sviluppo delle nuove tecnologie, con attenzione alla salvaguardia degli investimenti.

I Processi

Infine, dal punto di vista dei **Processi**, Cisco ha da tempo implementato delle policy interne a protezione di tutto il ciclo di vita di un prodotto/soluzione, in modo da mettere in sicurezza i propri Clienti, rendere robusti i propri prodotti e proteggere l'intellectual property di Cisco. Tale framework è chiamato **Trustworthy Systems**.

Abbiamo già descritto come il panorama delle minacce stia cambiando e gli avversari siano sempre più aggressivi. Nuovi attacchi sono realizzati da attori malevoli, con attività di contraffazione e prodotti manomessi.

Lo sviluppo sicuro di architetture, prodotti e applicazioni deve essere supportato da una completa gestione della supply chain, standard di sicurezza, gestione degli incidenti informatici, nonché dalla collaborazione con gli altri soggetti del settore.

Sistemi affidabili devono basarsi su tecnologie hardware, software e firmware integrati e verificabili, sicuri dal concepimento del prodotto fino alla disponibilità sul mercato, aderendo ad un ciclo di sviluppo sicuro che sia ripetibile e dimostrabile.

Cisco Secure Development Lifecycle prescrive e regolamenta questo metodologia, proprio con lo scopo di considerare gli aspetti di sicurezza sin dall'inizio, minimizzando le vulnerabilità durante lo sviluppo ed incrementando la resilienza delle soluzioni ad attacchi informatici.

Sistemi affidabili devono inoltre aderire a standard internazionali di certificazione, aiutando i Clienti ad acquisire soluzioni standard, con garanzia di performance e funzionalità, compatibili ed interoperabili con l'infrastruttura esistente.

Cisco supporta le certificazioni Common Criteria e Federal Information Process Standard (FIPS) 140--2

Cybersecurity, Cyber Forensics e Digital Forensics: stato, evoluzioni ed attività dell'Arma dei Carabinieri

Ten. Col. Marco Mattiucci
RaCIS Carabinieri

Il Dipartimento della Difesa americano, nel 2001, ha riportato la seguente definizione di *"cyberspace"*: *"il Cyber Space è un dominio globale all'interno del più ampio universo dell'informazione, e che consiste in una rete interdipendente di infrastrutture informatiche, internet compresa, reti di telecomunicazione, sistemi informatici, processori e controller dedicati"*. È bene tenere a mente le definizioni ufficiali di riferimento e soprattutto farle proprie nel momento in cui i fenomeni vengono analizzati altrimenti si corre il rischio di affidarsi ad una significazione tipica dei mass media anche quando devono essere prese delle decisioni di carattere strategico ed operativo nel settore.

Innanzitutto il *"cyberspace"* è ormai da tempo uno dei principali *"global commons"*, va quindi inquadrato tra i più comuni beni condivisi internazionalmente nell'ambito di: oceani, atmosfera, spazio esterno, regioni polari, ecc.. Questo vuole dire che dovrebbe essere soggetto a dei trattati internazionali in relazione al suo impiego, sfruttamento o navigazione. Molto semplicemente, ad oggi, lo spazio virtuale di Internet (corretta traduzione di *"cyberspace"* in italiano) è acceduto senza regole o restrizioni specifiche che non siano quelle delle singole giurisdizioni o stati nazionali da cui ipoteticamente l'accesso diparte.

Lo spazio virtuale di Internet (la "I" maiuscola è obbligatoria in quanto "internet" può indicare una qualsiasi rete basata sul protocollo IP – Internet Protocol – mentre Internet è la Rete delle reti connesse a livello mondiale ed è solo una) è il risultato dell'interconnessione di un grande e dinamico numero di infrastrutture informatiche e telematiche a svariati livelli di complessità in ogni area del mondo. Esso include 3 tipi fondamentali di risorse assolutamente distribuite: elaborazione, memoria e comunicazione.

Per meglio puntualizzare quanto appena espresso lo spazio virtuale di Internet non è solo *"spazio"* nel senso di luogo dove poter depositare dati (memoria). Il *"cyberspace"* è in grado anche di elaborare dati e di muoverli in ogni punto della terra come se si trattasse di un gigantesco sistema di elaborazione grande quanto il pianeta. Le risorse nello spazio virtuale, data la loro eterogeneità e per coerenza con le teorie delle reti di comunicazione, sono spesso chiamate *"servizi"*. Qualsiasi sistema connesso ad Internet genera dei servizi e ne sfrutta altri, i nodi che a qualsiasi titolo generano i servizi sono denominati classicamente *"server"*.

Analizzato in dettaglio il concetto di spazio virtuale su Internet si può passare ora a considerare quello di arma virtuale o arma digitale (*"cyber weapon"*): *"sistema digitale hardware e/o software operante nel cyberspace ed in grado di condurre dei cyber attack su target specifici"* . Questa definizione, volutamente generica, si focalizza sul concetto di *"cyber attack"* e non, come comunemente accade per l'argomento, su quello di risultato dell'attacco. Si vuole intendere che l'arma digitale non necessariamente è tale solo perché determina risultati catastrofici e su larga scala. Un sistema specificamente pensato per condurre attacchi in Internet a qualsiasi tipo di nodo o servizio (a prescindere dall'importanza) è di per se già potenzialmente un'arma che diviene pienamente tale quando consente ad un utilizzatore di "mirare", ossia di stabilire un target più o meno grande.

Dato che un *"cyber attack"* è: *"qualsiasi tipo di manovra offensiva perpetrata mediante sistemi digitali (cyber weapon(s)) a danno di uno o più sistemi informatici o telematici al fine di modificarli ad arte, penetrarne le protezioni, acquisirne informazioni o distruggerne le funzionalità ed i servizi"* rientrano nella definizione di arma virtuale o digitale anche la maggioranza dei virus e trojan attualmente esistenti ed operanti su Internet.

Il punto fondamentale ora è il passaggio dal concetto di arma virtuale a quello di guerra digitale (*"cyberwar"*): quando si determina una guerra digitale? O meglio la prima domanda da porsi è: *"quando un cyber attack può essere definito un atto di guerra digitale?"*. A questa domanda non esiste ancora una risposta a livello internazionale. Ci si è rifugiati dietro l'idea di infrastruttura critica valutando le risultanze dell'attacco, per cui se l'atto in se va a rimuovere dei servizi di natura fondamentale a livello sociale, energetico, finanziario, ecc. tali da mettere in pericolo delle grandi strutture allora si va a valutare il suo aspetto militare come atto di guerra. In tutto questo sfugge il concetto di attacco diretto ad una struttura militare di importanza anche non strategica. Se ciò avviene ad esempio da parte di una forza straniera identificabile pienamente va sicuramente considerato il suo aspetto come atto di guerra e non semplicemente come atto di intrusione da parte di un'organizzazione "pirata".

PUNTUALIZZAZIONI SUI CONCETTI DI CYBER-DEFENSE & CYBER-FORENSICS

È molto interessante analizzare in dettaglio i termini *"cyber-defense"* e *"cyber-forensics"* perché rende conto dell'ampio ventaglio di attività che a livello sia militare che civile possono essere poste in essere in questi settori.

La difesa in ambito virtuale, su Internet, è l'insieme delle strategie e delle misure da impiegare per la prevenzione e/o repressione di *"cyber attack"* e quindi:

(a) *"Intelligence"*: azioni preventive agli attacchi come intrusioni nei sistemi del "nemico" e/o analisi di dati circolanti;

(b) *"Security"*: individuazione, blocco e tracciamento degli attacchi;

(c) *"Counter-attack"*: uso legittimo delle cyber weapons contro precisi obiettivi individuati come "nemici".

La *"forensics"* in ambito virtuale è l'insieme delle metodologie, procedure e strumenti che permettono di acclarare tutte le fonti di prova inerenti un attacco informatico in corso di svolgimento o già svolto qualora se ne ravveda un chiaro aspetto di illegalità nel senso del codice penale e conformemente al codice di procedura penale del luogo considerato.

In definitiva la *"cyber-defense"* ha aspetti fortemente militari ed opera sempre al limite delle possibilità legali mentre la *"cyber-forensics"* opera solo entro precisi dettami legali ma ha necessità che sia definito un reato (in progressione o già avvenuto).

Se si vanno a considerare i punti (a),(b) e (c), infatti, non è difficile capire che l'azione di intelligence (a) può facilmente scaturire in intrusioni non autorizzate a sistemi "sotto osservazione" oppure in intercettazioni telematiche abusive (entrambi reati previsti dal codice penale italiano). Lo stesso dicasi per (c) in cui l'uso legittimo delle armi virtuali non solo non è regolamentato ma andrebbe a configurare ulteriori reati classicamente previsti dal nostro codice penale. Solo (b) sembra rimanere entro i limiti della legalità nella maggioranza dei casi ed infatti la *"cyber-security"* è ciò che apertamente tutti i grandi sistemi informatici in Italia prendono sicuramente in considerazione (mentre ci si guarda bene dal citare le proprie possibilità negli ambiti (a) e (c)).

L'uso di (a) e (c) sembra essere infatti peculiare di un ambito di guerra esattamente come avviene per la guerra elettronica (introdursi nel sistema "nemico", carpirne informazioni, modificarlo ad arte ed eventualmente distruggerlo è piuttosto comune e giustificato in questo ambito).

L'ARMA DEI CARABINIERI ED IL DIGITAL FORENSICS

L'Arma dei Carabinieri, come Polizia Giudiziaria in ambito sia militare che civile, ha profuso sforzi di adeguamento soprattutto nell'ambito del *"Digital Forensics"*, la versione più ampia e completa della *"cyber-forensics"* (quest'ultima si concentra su Internet e le reti): *"…the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions…"* [2009 "Advances in Digital Forensics V" – IFIP].

In particolare, a seguito degli aspetti di procedura penale legati a queste delicate attività tecniche di indagine, sono state fatte precise distinzioni in base ai tempi:

(i) *"Digital Investigation"*: attività spesso di iniziativa e generalmente preventiva rispetto al reato, il cui target non è il dibattimento ma il dimostrare che qualcosa di illecito sta avvenendo o è avvenuto per poi proseguire con degli approfondimenti;

(ii) *"Digital Forensics"*: azione altamente tecnica e solo post-mortem in cui l'autorizzazione a procedere della A.G. è elemento essenziale ed il cui target è precisamente il dibattimento ossia dimostrare dei fatti al fine di poter individuare ed incriminare definitivamente un indagato.

Nel caso (ii) tutto deve sempre essere accuratamente documentato e dimostrato attraverso processi logici accettabili dalla comunità scientifica di settore nel tempo in cui gli accertamenti scientifici sono svolti. Nel caso (i) il rigore scientifico lascia posto all'intuito ed alla capacità di correlare più fatti sia tecnici che di contesto al fine di poter sviluppare delle ipotesi magari successivamente meglio dimostrabili tramite (ii).

Il Reparto Tecnologie Informatiche del Ra.C.I.S. si occupa prevalentemente di (ii) in ambito elettronico ed informatico facendo dell'altissima specializzazione dei suoi operatori l'elemento fondamentale per portare poi i referti in dibattimento, mentre il Reparto Indagini Tecniche del R.O.S. può spaziare sia in (ii) che in (i) avendo come punto di forza la sua possibilità di proiezione verso l'esterno e sul campo in ambito high tech.

I tipici argomenti trattati dal "Digital Forensics" nell'ambito specialistico del Reparto Tecnologie Informatiche sono:

- Computer forensics: repertamento ed analisi di memorie digitali;
- Mobile forensics: repertamento ed analisi di sistemi cellulari ed annessi servizi;
- Network forensics: repertamento ed analisi di sistemi virtuali su Internet e sulle reti;
- Data Base & Softwar Forensics: repertamento ed analisi di software e database;
- Embedded System Forensics: repertamento ed analisi di sistemi elettronici speciali sia integri che danneggiati fisicamente.

STANDARD DI RIFERIMENTO PER LA DIGITAL FORENSICS

Il Reparto Tecnologie Informatiche del Raggruppamento CC Investigazioni Scientifiche basa la sua attività sulle seguenti fonti di standardizzazione a livello internazionale:

1) Europol / Cepol: centri di addestramento e studi per i crimini che coinvolgono l'high tech.
2) ENFSI-FITWG: Forensic Information Technology Working Group dell'European Network of Forensic Science Institutes – gruppo di lavoro delle FFPP a livello internazionale che si occupa degli high tech crime.
3) Linee guida ISO/IEC:

a. ISO/IEC 27037:2012 *"Guidelines for identification, collection and/or acquisition and preservation of digital evidence"*
b. ISO/IEC 27041 (WD) *"Guidance on assuring suitability and adequacy of investigation methods"*
c. ISO/IEC 27042 (WD) *"Guidelines for the Analysis and Interpretation of Digital Evidence"*
d. ISO/IEC 27043 (WD) *"Guidance on Investigation Principles and Processes"*
e. ISO/IEC 27035:2011 *"Incident Management"*

La documentazione citata è continuamente soggetta ad aggiornamenti e revisioni, ciò a seguito di periodici incontri e seminari a livello internazionale di settore sia di FFPP che di specialisti privati.

LA FRONTIERA DELLA DIGITAL FORENSICS

La *"Digital Forensics"* è ad oggi elemento fondamentale per la "*cyber-defense"* in quanto sviluppabile in precisi e protetti ambiti legali che la rendono prontamente fruibile in ambito non di guerra. Ad ogni modo l'esperienza dei tecnici in tale settore è oltremodo utile anche nel caso in cui si dovessero mettere in piedi dei meccanismi di protezione o attacco "cyber" in ambito bellico. Questa neo-scienza ha enormi possibilità e diverse linee di ricerca ma ovviamente ha anche dei precisi limiti di sviluppo. È importante citarne alcuni per far capire quali siano le direzioni di crescita della materia:

- Attività a "cuore aperto" sui sistemi elettronici ed informatici durante o appena dopo il reato (triage);
- Raccolta dei dati a "caldo" nel mentre si formano o modificano;
- Individuazione e raccolta di dati temporanei che si presentano in rete solo per pochi istanti;
- Osservazione della memoria centrale (RAM) senza modifica o intrusione nella stessa;
- Attività di indagine da "remoto" su macchine autorizzate o protette;
- Attività di controllo remoto di dispositivi elettronici e telematici mediante agenti software;
- Superamento delle barriere generate dalla counter-forensics e dai cloud system;
- Superamento, per scopo di PG, delle barriere di privacy degli utenti (es. password, cripto, ecc.).

Si tratta di limiti difficili da valicare ma anche di intriganti mete di ricerca scientifica che determineranno, una volta superati, nuovi ed interessanti metodi di indagine. Va ribadito, in questo senso, che tali innovativi strumenti di indagine andranno a formare, quasi per certo, nuove tipologie di possibili cyber-weapons che, opportunamente adattate a tale scopo, risulteranno di estrema efficacia in un eventuale impiego bellico

Application Delivery Controller

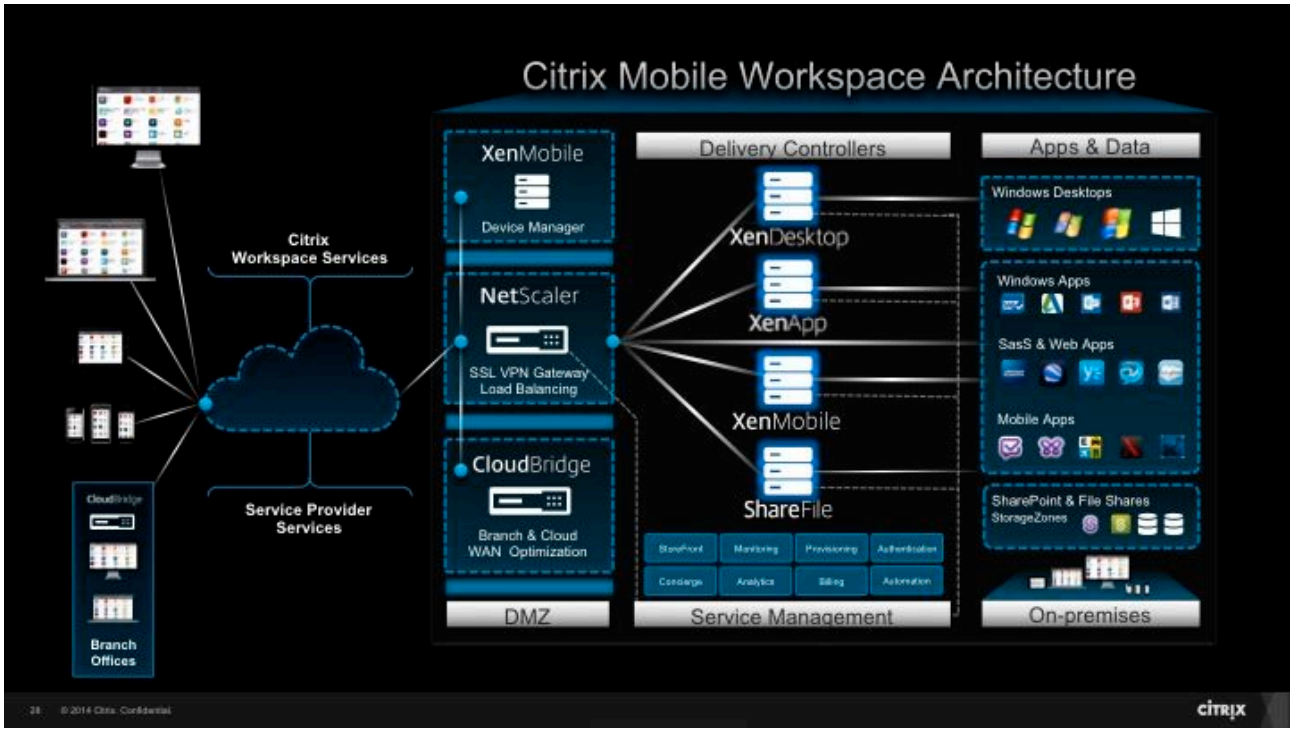
David Cenciotti
Systems Engineer, Cloud Networking Group
Citrix Systems

Gli Application Delivery Controller (ADC) svolgono un ruolo fondamentale nella protezione delle organizzazioni dai cyber attack e più specificatamente degli attacchi Denial of Service.

Oltre a garantire la distribuzione del traffico sui sistemi situati nel datacenter (o distribuiti su più siti), in base a logiche di prossimità, carico o stato della rete, gli ADC ottimizzano le performance dei server e delle applicazioni di Back End (ovvero di quell'area di un'applicazione non visibile direttamente agli utenti poiché preposta alla generazione e alla modifica dei contenuti, anche mediante accesso ai database) dei quali verificano continuamente lo "stato di salute". Ma non solo.
Gli ADC di nuova generazione hanno piena visibilità (fino al livello 7 della pila ISO/OSI) del traffico e del relativo contesto applicativo, e dispongono dell'intelligenza e delle capacità necessarie per identificare e mitigare gli attacchi, discriminando tra utenti legittimi e attaccanti.

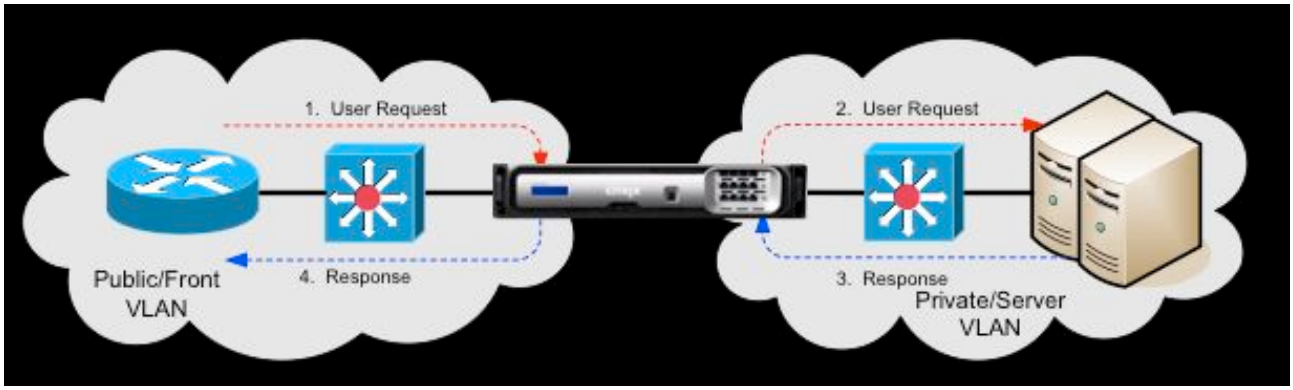
Gli Application Delivery Controller sono dei sistemi, fisici, virtualizzati o piattaforme "multi-tenant" (cioè appliance fisiche sulle quali è possibile istanziare diverse macchine virtuali), che rappresentano l'evoluzione dei tradizionali Load Balancer (Bilanciatori di Carico). La loro funzione di base è quindi quella di prendere in carico il traffico destinato alle applicazioni situate nel Back End della rete e distribuirlo sui server di destinazione in base a criteri di carico, raggiungibilità, performance della rete o contenuto. In pratica, il loro compito primario è garantire la continuità di un servizio verificando che i sistemi informatici preposti ad erogarlo siano in grado di farlo. Qualora, per un qualsiasi motivo, il server o l'applicazione di Back End non soddisfino uno dei criteri previsti dall'amministratore, l'ADC provvederà a ridirigere le richieste dei client solo verso quei sistemi in grado servirle; un processo del tutto trasparente ai client, ma fondamentale per evitare anche le più brevi (ma costosissime) interruzioni di servizio.
Nel corso degli anni, in virtù della loro centralità nell'ambito della distribuzione del traffico, gli ADC hanno acquisito ulteriore "intelligenza" concentrando una moltitudine di ruoli e di funzioni, anche inerenti alla sicurezza, tra cui: Health Monitoring; SSL Offloading, Bridging e Proxying;

VPN SSL Concentrator, Caching (Integrated o per mezzo di redirection verso un cache engine esterno); GSLB (Global Server Load Balancing); Link Load Balancing; Content Switching; Content Filtering; WAF (Web Application Firewall); Surge Control; Denial of Service Protection; TCP Optimization (Multiplexing, SACK, MTU discovery, ecc.); L2 Extension. Inoltre, gli ADC svolgono l'importante ruolo di Front End per l'accesso a tutte le soluzioni di Application & Desktop Virtualization, Access and Data Security, Data Sharing ed Enterprise Mobility Management.



Come funziona un ADC

Finora si è parlato di ADC principalmente in termini di feature rese disponibili; tuttavia, conoscere i principi di funzionamento di questi sistemi è utile per comprenderne il vero valore aggiunto nel contrasto e nella mitigazione degli attacchi.
In una configurazione-tipo, a livello di architettura logica, un ADC risiede tra i client e i server da bilanciare, comportandosi da transparent proxy: i client terminano le sessioni sull'ADC che a sua volta che, a sua volta, instaurerà nuove sessioni verso i server di backend. In questa maniera, del tutto trasparente ai client - che crederanno di "parlare" direttamente con i server - viene spezzata la comunicazione tra quello che potremmo considerare l'"esterno" della rete e il "cuore" della stessa, dove sono presenti gli applicativi e i database: tutto il traffico passa per il bilanciatore, che una volta effettuate le verifiche previste, lo inoltrerà verso le reali destinazioni.

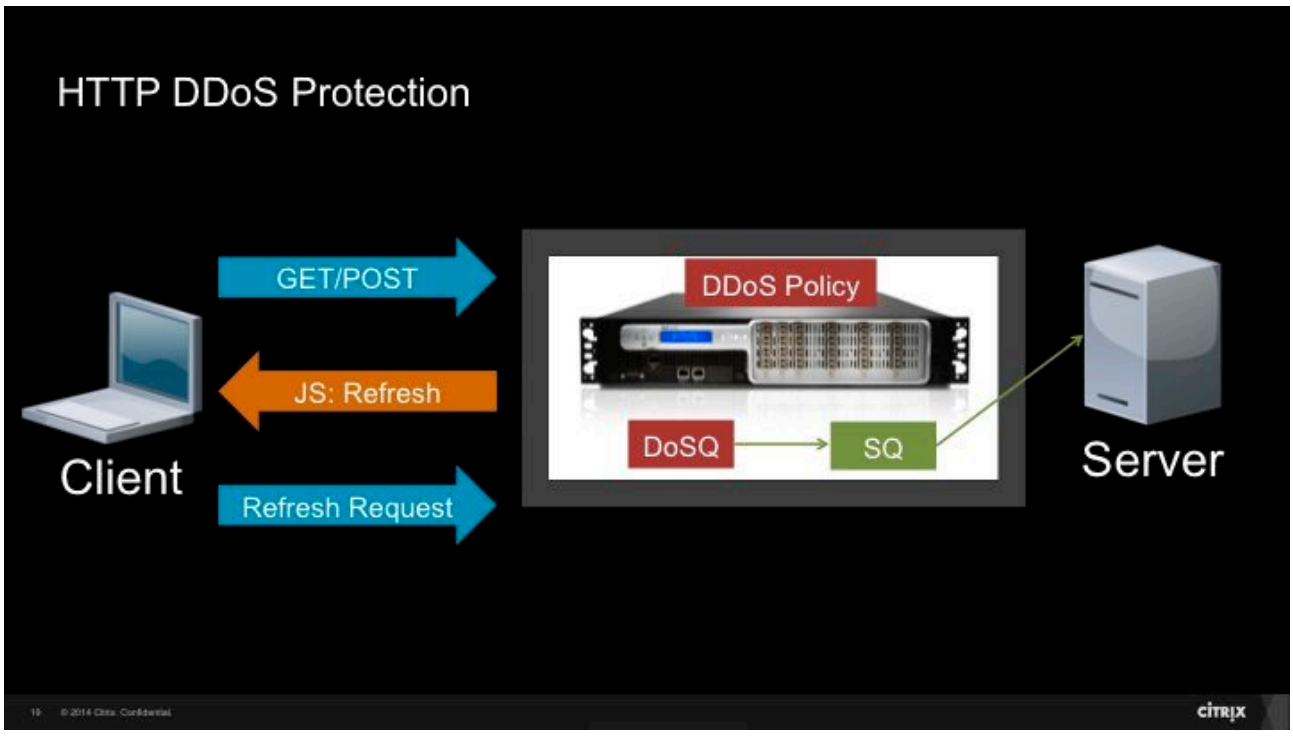


Come già accennato, per garantire agli utenti la fruizione del servizio senza soluzione di continuità, l'ADC monitorizza costantemente lo stato di salute del pool di sistemi di destinazione. Tale processo avviene mediante il monitoraggio dei servizi. Il Monitoring consiste nell'utilizzazione di tutta una serie di controlli (detti monitor o probe) per determinare se un sistema sia in grado di gestire il traffico e quindi debba essere mantenuto nel novero di quelli verso i quali l'ADC gira il traffico. I monitor più comuni sono il Ping, che verifica la raggiungibilità di rete del server mediante pacchetti ICMP, e il TCP, che prevede l'esecuzione della prima parte di un three-way handshake tra l'ADC e il server di Back End, terminato prima che la sessione TCP sia stabilita e che serve per "certificare" la capacità del sistema di accettare nuove sessioni. Ma ne esistono ovviamente anche di più complessi, come quelli che permettono di effettuare delle verifiche sul contenuto del codice HTML di una pagina Web, o quelli che attraverso trap SNMP verificano il carico CPU della macchina di destinazione per rilevare eventuali, rischiose, sofferenze. Generalmente, i vari monitor resi disponibili dall'ADC sono aperti a personalizzazioni anche piuttosto spinte, necessarie ad adattarli allo specifico comportamento di un'applicazione mentre, per le realtà applicative più complesse, è possibile combinare i monitor attribuendo agli stessi pesi differenti al fine di definire metriche di tipo "custom" su cui basare le decisioni di distribuzione del traffico. È addirittura possibile verificare l'health state di un sistema attraverso l'esecuzione di uno script lanciato dal bilanciatore.
E' proprio il processo di monitoring a conferire all'Application Delivery un ruolo fondamentale nell'ambito della sicurezza di un'infrastruttura informatica.

Il ruolo degli ADC in ambito Security

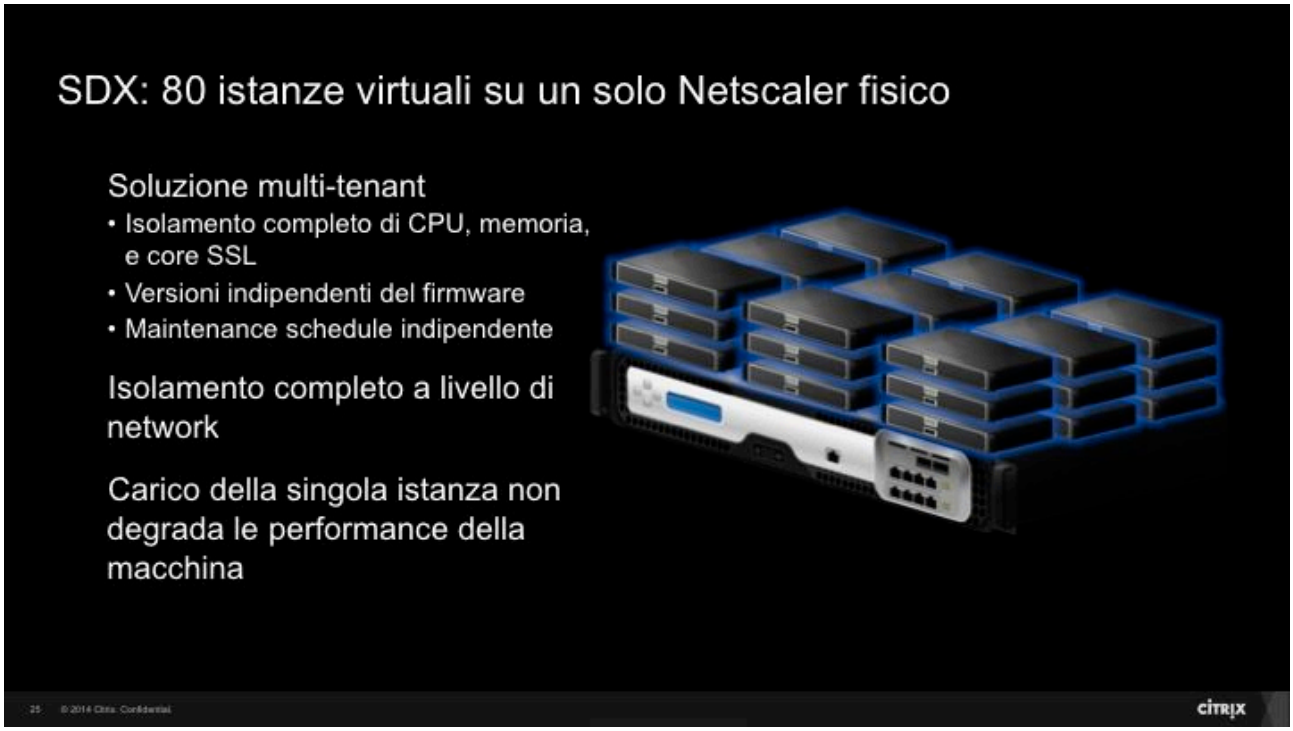
Sia ben chiaro, un bilanciatore non può sostituire strumenti di security dedicati. Tuttavia, in virtù delle proprie modalità operative, fornisce un considerevole valore aggiunto in caso di attacco cibernetico integrandosi con il resto dell'architettura di sicurezza. Difatti, l'ADC è l'unico "oggetto" all'interno della rete che interroga continuamente i server e le applicazioni di Back End, prendendo decisioni anche sulla base del risultato dell'health check eseguito sugli stessi. Firewall, IPS (Intrusion Prevention System) e altri sistemi normalmente preposti alla protezione da attacchi dall'esterno e dall'interno della rete, non verificano lo stato dei sistemi, ma normalmente si limitano a validare il traffico diretto agli stessi. L'ADC, oltre ad essere lo strumento con funzioni di sicurezza più "prossimo" al cuore della rete, agisce direttamente su traffico che gestisce sulla base delle politiche impostate, sull'esito dell'inspection e soprattutto sullo stato di salute dei server. Pertanto, oltre a poter mitigare attacchi dovuti al traffico malevolo degli attaccanti è in grado di proteggere i sistemi critici di un'organizzazione, anche da DoS in un certo senso involontari, ovvero causati da overload di traffico lecito. Senza dimenticare che il concetto di bilanciamento fu introdotto proprio per garantire la continuità del servizio a livello di server farm o distribuito su scala geografica (mediante GSLB), e rendere l'infrastruttura più resiliente ai fault o alle temporanee indisponibilità delle applicazioni (per attacchi o avarie).
Inoltre, tradizionalmente, in contesti che richiedono maggiore capacità elaborativa, gli ADC sono utilizzati proprio per bilanciare il carico verso batterie di Firewall poste a protezione delle isole applicative o dei CED, divenendo, di fatto, veri e propri "abilitatori" della stessa infrastruttura di sicurezza.
Il ruolo del bilanciatore nella protezione dei sistemi si è reso ancora più importante con l'introduzione di ulteriori feature di sicurezza come il WAF, l'HTTP DDoS Protection e il Surge Control corredati da vari strumenti di visibility e reporting.
Il Web Application Firewall è il firewall applicativo che filtra il traffico dei servizi Web, ovvero HTTP, HTTPS e XML. Alcuni ADC hanno a bordo un WAF che implementa un security model ibrido, ovvero basato su un motore di apprendimento delle caratteristiche dell'applicazione secondo

il “modello di sicurezza positivo”, per la protezione dagli “zero day”, ed un set di alcune migliaia di signature (“modello di sicurezza negativo”) per la protezione dagli attacchi noti. Per quel che concerne il motore di apprendimento, l’engine rileva automaticamente il comportamento lecito ed atteso per ciascuna applicazione o servizio al fine di proteggere le Web Application da diversi vettori di attacco quali: SQL Injection, Cross Site Scripting, CSRF (Cross Site Resource Forgery), Buffer Overflow, Cookie Tampering, Forceful Browsing, Web Form Security e, per quanto riguarda l'XML: XSS, SQL Injection, Malicious code or objects, Badly-formed XML requests, DoS.
Per quel che riguarda le signature, il WAF attinge alle firme degli attacchi (aggiornate in modalità automatica o manuale) del mondo Snort.
L’HTTP DDoS Protection è invece una funzionalità che si basa sull'invio di un javascript ai client che forza il refresh della pagina e il settaggio di uno specifico cookie, la cui presenza determina l’inoltro o meno verso i portali protetti. In pratica, raggiunta una determinata soglia di sessioni HTTP, l’ADC inizia a sondare i client in modo tale da verificare se il traffico verso i server è generato da utenti “umani”, ovvero browser che si presentano con il cookie corretto, o se si tratti di traffico registrato. Ovviamente, l’adozione di tecniche di DDoS mitigation non previene disservizi causati dalla saturazione dei link, nei confronti dei quali un ADC non sarebbe molto efficace. Tuttavia, abilitare questo tipo di controllo su un ADC consente di discriminare gli utenti leciti dai sistemi legati ad una botnet, per ridurre il carico sui sistemi di Back End e garantire la continuità del servizio per il tempo necessario ad adottare, lato carrier, ulteriori contromisure di contrasto. Sebbene possa sembrare poca cosa, scartare il traffico generato da bot e continuare ad erogare un servizio per qualche minuto in più potrebbe essere di vitale importanza per un’organizzazione (o per un intero paese) in caso di cyber attack. Ecco dunque spiegata la presenza di questo tipo di contromisura di sicurezza su un bilanciatore.



Un’altra funzionalità importante resa disponibile dai più avanzati ADC è il Surge Control. Attraverso la feature di Surge Protection, il bilanciatore permette di creare delle regole ad hoc per ritardare l'apertura delle nuove sessioni verso il Back End, in modo tale da consentire ai server di smaltire un po’ di traffico prima di prenderne in carico di nuovo. Questa tipologia di offloading (che si unisce all’offload dell’SSL, al caching e al multiplexing per alleggerire il carico sui server) è particolarmente utile in caso di DoS indotti da picchi di traffico (lecito) causati ad esempio dalla pubblicazione e successiva diffusione di un link ad un contenuto interno su social network o siti

d’informazione. Non essendo un attacco in senso stretto, il traffico generato dal contenuto “virale” passerebbe il controllo dei Firewall, facendo però collassare il Web Server preposto alla pubblicazione dello stesso. La presenza di un ADC con tale capacità permette di ovviare a questo problema, applicando un breve ritardo sull’apertura di nuove sessioni in base a tre modalità di gestione del sovraccarico di traffico: rilassato, moderato e aggressivo con ritardi incrementali.



Infine, non è da sottovalutare la possibilità di consolidare sull’ADC ulteriori funzionalità di sicurezza, attraverso l’integrazione di prodotti di terze parti ospitati come istanze virtuali di bilanciatori multi-tenant: si parla in questo caso di SDA, Software Defined Appliance, perfettamente integrabile in una moderna SDN (Software Defined Network).

Software Defined Network

Ai progressi in termini di capacità di calcolo e virtualizzazione si è a lungo opposta una certa rigidità della rete che rappresenta tuttora un ostacolo per la realizzazione di architetture di rete e cloud flessibili, scalabili e in grado di ottimizzare le performance delle applicazioni e la user experience degli utenti. I dispositivi di rete sono apparati fisici con capacità fisse, collegati secondo topologie statiche e con policy di accesso e sicurezza poco flessibili, e normalmente sono caratterizzati da una certa complessità di gestione: in altri termini, sono del tutto inadeguati ai moderni concetti di cloud-computing.
È questa la ragione per cui in ambito networking è stato sviluppato un nuovo paradigma architetturale che prende il nome di Software-Defined Network (SDN). In termini generici, l'SDN è una rete intelligente, in cui le applicazioni sono in grado di programmare gli apparati di rete per ottimizzare la distribuzione dei contenuti, grazie alla separazione sugli apparati stessi dei meccanismi di controllo dei flussi da quelli di instradamento del traffico (disaccoppiamento Control Plane e Data Plane). È indubbio che in virtù del ruolo centrale che rivestono nel delivery applicativo e della sicurezza, anche i moderni ADC debbano poter essere controllati e configurati da una SDN, in special modo se offrono servizi ad alto valore aggiunto come quelli brevemente descritti in questo articolo.