

SECURITY

& BUSINESS

n.29

CYBER ATTACK

LA SICUREZZA A RISCHIO PER IL RAPPORTO CLUSIT NUOVA EDIZIONE 2015

Ritorna l'aggiornamento autunnale del Rapporto Clusit presentato a Verona in occasione della tappa scaligera del Security Summit. Un rapporto sempre più ricco, come sottolinea il presidente onorario del Clusit, Gigi Tagliapietra, evidenziando i nuovi contributi al rapporto.

Nel 2015, infatti, oltre alle analisi egregiamente svolte dai gruppi di lavoro in seno al Clusit e al contributo rinnovato da parte di Fastweb, si registrano i con-



tenuti inediti di Akamai, di IBM, della Polizia Postale e delle Comunicazioni e del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza. Per l'edizione 2016, inoltre, sono previsti altri "ingressi", a cominciare da IDC, che con il Clusit ha siglato una partnership. **pag.04**

NEWS

TREND MICRO ACQUISISCE HP TIPPINGPOINT

L'azienda giapponese acquisisce uno dei fiori all'occhiello della sicurezza HP, portando nel proprio paniere d'offerta le funzionalità IPS e Firewall di nuova generazione della famiglia TippingPoint, inclusi i DVlabs e la Zero Day Initiative.

L'accordo, del valore approssimativo di 300 milioni di dollari, porterà alla creazione di una Network Defense business unit che avrà il compito di gestire più di 3.500 clienti enterprise. **pag.09**

NEWS

BT PROTEGGE I DATI DEL SETTORE FINANZIARIO CON IL SERVIZIO DI ETHICAL HACKING

Recenti ricerche mostrano come gli attacchi ai sistemi finanziari mondiali siano in continua crescita. I danni che possono derivarne in caso di successo sono potenzialmente enormi e tali da minare la fiducia degli investitori e dei correntisti. BT adotta i test di sicurezza certificati STAR di CREST per proteggere le organizzazioni finanziarie dalle crescenti minacce informatiche. **pag.10**

IN QUESTO NUMERO:

EDITORIALE

pag.03

• La resilienza nell'impari lotta per la sicurezza

CYBER ATTACK

pag.04-06

• La sicurezza a rischio per il Rapporto Clusit nuova edizione 2015

TENDENZE

pag.07

• Gartner vede la Security Governance maturare

NEWS

pag.09

• Trend Micro acquisisce HP TippingPoint

pag.10

• BT protegge i dati del settore finanziario con il servizio di Ethical Hacking

smau

Roadshow 2015



**Smau ti accompagna
nello sviluppo e nella crescita del tuo business
in qualità di partner di innovazione.**



Nell'anno di **Expo 2015** Smau varca i confini nazionali per creare nuove occasioni di networking a livello internazionale supportando la crescita e lo sviluppo dell'ecosistema dell'innovazione Italiano. Attraverso il suo Roadshow Smau rappresenta il partner di riferimento a supporto della **"digital transformation" delle imprese e delle pubbliche amministrazioni** facilitando l'incontro diretto con gli operatori dell'ecosistema digitale e ICT, il meglio delle startup italiane, importanti Università e Business School, le Associazioni dell'Industria e del Commercio e tutte quelle realtà che svolgono un ruolo fondamentale **per rilanciare l'economia italiana e l'innovazione made in Italy.**

Le tappe 2015:

BERLINO
12-13 marzo

PADOVA
1-2 aprile

TORINO
29-30 aprile

BOLOGNA
4-5 giugno

FIRENZE
8-9 luglio

MILANO
21-22-23 ottobre

NAPOLI
10-11 dicembre

Contatti |



+39.02.283131 |



info@smau.it |



www.smau.it |

La resilienza nell'impari lotta per la sicurezza



di Gaetano Di Blasio

La tappa di Verona ha chiuso l'edizione 2015 del Security Summit, la più importante manifestazione sulla sicurezza dei dati e dei sistemi informatici in Italia, organizzata dal Clusit con la collaborazione di Astrea. È stata l'occasione per aggiornare il Rapporto Clusit con i dati sugli attacchi relativi al primo semestre del 2015.

Il quadro è sempre più drammatico: il cyber crime è cresciuto del 30% nel primo semestre: a esso vanno ricondotti il 66% degli attacchi resi noti in questo periodo. Erano il 36% nel 2011. Rimandiamo a pagina 4 per l'aggiornamento dei dati.

Di fatto, la situazione è sconcertante: Andrea Zapparoli Manzoni, membro del consiglio direttivo del Clusit e tra gli autori del Rapporto, sottolinea quanto impari sia la guerra ai cyber criminali con una metafora "medievale": «Costa meno all'attaccante alzare le scale di quanto costa al castellano alzare le mura».

Il sempre più florido mercato dell'hacking as a service amplifica il fronte di attacco, che non è più solo costituito dai programmatori superspecializzati che sviluppano applicazioni maligne. Ma non solo, perché ormai gli strumenti di attacco sono sempre più automatizzati. Ci sono sniffer o altri bot che scandagliano la Rete alla ricerca di vulnerabilità e riescono a farlo in tempi rapidissimi.

Questo significa che bisogna cambiare prospettiva e molte imprese stanno cominciando a capirlo, merito anche dell'eco mediatica che la crescente mole di attacchi genera (per quanto l'impressione è che quelli noti siano una minoranza). In pratica occorre chiedersi "cosa fare quando sarò attaccato", dando per scontato che ciò accadrà prima o poi.

Ci sono best practice per l'incident response, ma la dinamicità con cui occorre confrontarsi rende difficile organizzarsi per la maggior parte delle aziende che non dispongono di un team per la sicurezza.

I partecipanti alla tavola rotonda del Security Summit di Verona hanno provato a elencare alcune delle contromisure che è utile mettere in atto per cercare di raggiungere quello che è appare l'unico obiettivo possibile: la cyber resilience. La capacità di riprendersi dopo l'attacco è fondamentale: un po' come la spiga che si piega ma non si spezza.

Numero 29
Tutti i marchi sono registrati
e di proprietà delle relative
società

Registrazione al tribunale
n.585 del 5/11/2010

Editore: Reportec srl

Direttore responsabile:
Gaetano Di Blasio

In redazione: Riccardo Florio,
Giuseppe Saccardi, Paola
Saccardi

Immagini: dreamstime.com -
www.securitybusiness.it

Reportec

SECURIT
& BUSINESS

La sicurezza a rischio per il Rapporto Clusit nuova edizione 2015

di Gaetano Di Blasio

Cresce la pressione del Cybercrime che pesa per il 66% degli attacchi, ma in Italia è peggio, mentre sorgono nuovi fronti di attacco a cominciare dall'IoT. Il Security Summit apre il mese della sicurezza a Verona

Consueto aggiornamento autunnale del Rapporto Clusit presentato a Verona in occasione della tappa scaligera del Security Summit. Un rapporto sempre più ricco, come sottolinea il presidente onorario del Clusit, Gigi Tagliapietra, evidenziando i nuovi contributi al rapporto.

Nel 2015, infatti, oltre alle analisi egregiamente svolte dai gruppi di lavoro in seno al Clusit e al contributo rinnovato da parte di Fastweb, si registrano i contenuti inediti di Akamai, di IBM, della Polizia Postale e delle Comunicazioni e del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza. Per l'edizione 2016, inoltre, sono previsti altri "ingressi", a cominciare da IDC, che con il Clusit ha siglato una partnership.

L'evento, organizzato dall'associazione di professionisti della sicurezza in collaborazione con Astrea presso l'hotel Crowne Plaza Verona Fiera, ha aperto in Italia il mese europeo della sicurezza informatica, cioè l'European Cyber Security Month, campagna dell'Unione Europea, organizzato dall'agenzia europea ENISA e supportata nel nostro Paese dal Clusit.

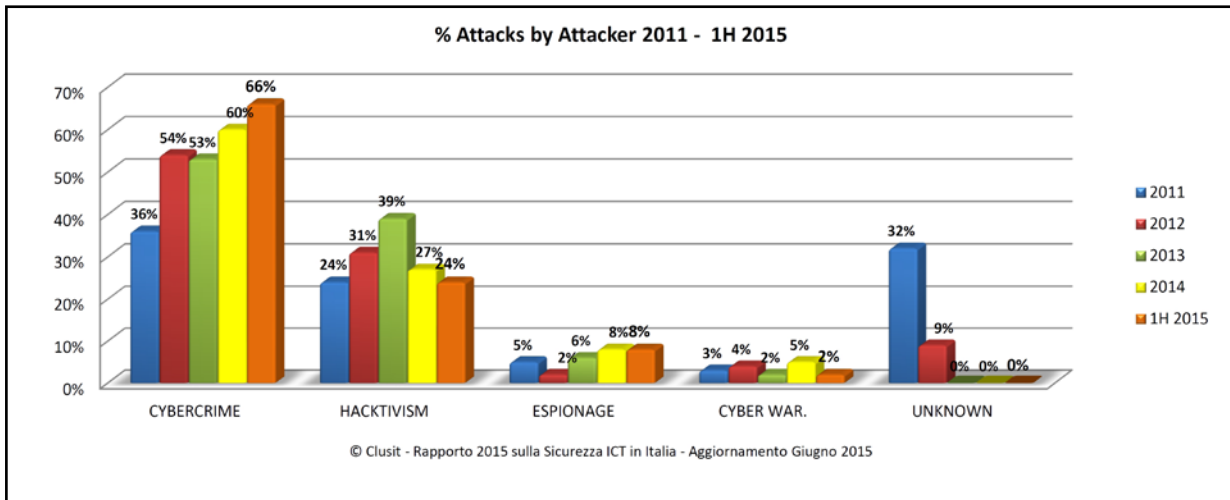
Un mese in cui è fondamentale l'opera di sensibilizzazione e nulla di meglio, per questo dell'analisi su-

gli attacchi del primo semestre 2015, che aggiornano il Rapporto. Quest'ultimo, inoltre, viene redatto dal 2011, per cui comincia a esserci uno storico interessante, che consente alcune valutazioni temporali. In 54 mesi dalla prima edizione, gli esperti del Clusit hanno classificato come gravi, in media, 88 incidenti al mese, ogni mese. Nel primo semestre 2015 sono stati 86 al mese, ma valutati con nuovi criteri di classificazione (per esempio vengono esclusi i defacement fino allo scorso anno considerati gravi, ma oggi privi d'impatto), introdotti per allinearli al livello crescente delle minacce.

I nuovi criteri hanno determinato una riduzione del numero assoluto di attacchi gravi presi in considerazione nel 2014 (altrimenti ci sarebbe registrato un aumento del 10%), ma nel primo semestre 2015, pur applicando i nuovi criteri, la crescita rispetto al primo semestre 2014 è del 15%.

Gli highlights sulle minacce

Rapidamente evidenziamo i principali dati emersi, cominciando dall'ulteriore aumento del cybercrime, che



è stato identificato quale responsabile del 66% degli attacchi noti gravi, avvenuti nei primi sei mesi dell'anno. Questo a livello globale, ma in Italia potrebbe essere anche molto peggio, considerate le misurazioni sulla rete di Fastweb, che ha analizzato 5 milioni di eventi, attribuendo al cybercrime il 93% degli attacchi 2014 (dato sostanzialmente confermato nei primi sei mesi 2015 con il 92,2%).

Volendo guardare il bicchiere mezzo pieno, va detto che questa pressione ha prodotto una maggiore consapevolezza dei rischi e dell'ineluttabilità degli attacchi. Ciò non toglie che la maggior parte delle imprese italiane non si accorgono di essere state attaccate e, quando lo scoprono è con molto ritardo. Il risultato sono danni in Italia da incidenti e disastri per 9 miliardi di euro in un anno, come spiega Andrea Zapparoli Manzoni, membro del Clusit tra gli autori dell'analisi sugli attacchi.

Sempre Zapparoli sottolinea l'emergere di nuove minacce che riguardano ambiti specifici, quali l'automotive (con accessi all'elettronica di bordo e ai dispositivi in tasca ai passeggeri tramite Bluetooth), l'entertainment (con le funzioni delle console di videogame sfrut-

tate a scopi malevoli) e, più in generale, l'Internet of Things o, meglio, l'Internet of Hacked Things. Presi di mira con continuità nel 2015 aziende dei settori telecomunicazioni e Grande Distribuzione Organizzata.

Interessante il dato osservato sulla rete di Fastweb (oltre 6 milioni di indirizzi IPv4): dopo il boom del 2014, gli attacchi DDoS sono calati nei primi sei mesi del 2015 in numero, volume e durata, afferma Davide Del Vecchio, responsabile del SOC di Fastweb.

Pierluigi Rotondo di IBM, invece, tra le risultanze delle analisi sulle minacce, segnala il netto miglioramento delle tecniche di evasione registrato in tutti i malware. Si tratta di tecnologie, per esempio di mascheramento, che consentono di eludere i controlli da parte dei sistemi per la sicurezza, quali antivirus ma anche firewall e IPS (Intrusion Prevention System).

Oltre gli attacchi

Il Rapporto contiene anche molto altro non direttamente connesso con gli attacchi e le minacce e, in particolare, i sempre più numerosi "Focus On" di approfondimento, tra cui quelli sui temi dell'Internet of Things, M-Commerce e i Bitcoin, con aspetti tecnici e

CYBER ATTACK



legali della criptovaluta, nonché sulla doppia autenticazione per l'accesso ai servizi di posta elettronica. Altri contenuti del report brevemente presentati a Verona hanno riguardato: la sicurezza dei siti Web appartenenti alla Pubblica Amministrazione; il regolamento generale sulla protezione dei dati, con le novità per i cittadini, le imprese e le istituzioni; le tematiche legali relative al cloud e alla sicurezza; il Return on Security Investment; l'impatto della Direttiva 263/agg.15 di Banca d'Italia sugli operatori del settore bancario.

Molti di questi temi, insieme agli attacchi, hanno alimentato la discussione nella sessione plenaria, con una tavola rotonda moderata da Tagliapietra, con la partecipazione, oltre che di Zapparoli, Del Vecchio, Rotondo, anche di Stefano Pasquali, responsabile

dell'unità organizzativa Comunicazione Informatica del Comune di Verona, Alberto Mercurio Referente Tecnologie Digitali UNIS&F (Unindustria Servizi & Formazione Treviso Pordenone); Roberto Tarocco, Regional Account Manager di Trend Micro, Matteo Perazzo di DiGi International.

Piuttosto allarmante il quadro della situazione sotto tutti i punti di vista, basti ricordare il commento tranchant di Mercurio: «La consapevolezza c'è, ma si agisce solo quando accade qualcosa grave». Insomma, una nazione alla mercé dei cyber criminali. In pillole gli ingredienti per una cura essenziale espressione della tavola rotonda: cyber resilience, sharing delle informazioni, prevenzione, controllo continuo delle pratiche basilari per la sicurezza e ancora tanta cultura in azienda su tutti i dipendenti.



DIVENTA PARTNER KASPERSKY



PROPONI LE MIGLIORI SOLUZIONI IT

per aziende di tutte le dimensioni ed esigenze



AUMENTA IL TUO FATTURATO

con costanti guadagni e margini più alti



PARTECIPA AD UN ESCLUSIVO PROGRAMMA DI INCENTIVI

che riconosce la tua fedeltà e il successo come nessun altro



REGISTRATI SU WWW.KASPERSKYPARTNERS.EU

Gartner vede la Security Governance maturare

L'indagine annuale su privacy, IT risk management, business continuity e compliance, condotta dagli analisti di Gartner, rileva una maggiore attenzione alla sicurezza, grazie al crescente impatto del digital sul business e a una più alta risonanza degli incidenti di sicurezza

Le procedure per la gestione della sicurezza stanno maturando, secondo i risultati di un'indagine realizzata dagli analisti di Gartner tra febbraio e aprile 2015, coinvolgendo 964 figure presso grandi imprese (minimo 100 dipendenti) in 7 nazioni.

In particolare, la ricerca annuale di Gartner su privacy, IT risk management, information security, business continuity e compliance, spiega Tom Scholtz, vice president e Gartner Fellow, mostra che la consapevolezza verso la sicurezza è aumentata perché si è compreso il valore dell'impatto del rischio in ambito digital sul business. Molto hanno contribuito i passaggi in cronaca di numerosi e significativi incidenti di sicurezza, avvenuti nel corso del 2014.

Il 71% degli intervistati ha dichiarato che i dati sull'IT risk management influenzano le decisioni in seno al consiglio di amministrazione. Fino a diventare parte della corporate governance. Questo diventa possibile specialmente laddove membri del team di sicurezza vengono ascoltati al di fuori del team stesso. Ciò avviene nel 38% delle imprese coinvolte.

In questi casi si riesce a superare l'idea, diffusa presso molti top manager, che la sicurezza sia un problema dell'IT. Un errore in cui cascano molti perché non sanno quanti degli incidenti di sicurezza sono causati dall'errore umano. In un crescente numero di imprese, però, il problema viene ricondotto al rischio aziendale. Per il 63% degli intervistati,



il team di sicurezza viene supportato da top manager esterni al team (era il 54% nel 2014). Rimane peraltro ferma al 30% la quota di CEO e membri del Cda che supportano direttamente la gestione della sicurezza (più precisamente era al 29% nel 2014).

Questi manager "illuminati" sono più diffusi in Europa Occidentale (63%) e in Asia/area del Pacifico (67%), rispetto al Nord America (57%).

L'invio degli analisti Gartner è dunque quello di coinvolgere un senior executive nella gestione della sicurezza, senza del quale sarà difficile essere realmente efficaci nel supportare le esigenze di business in termini di governance.

Purtroppo proprio l'efficacia delle policy di sicurezza è ancora scarsa, anche perché solo per il 30% degli intervistati la definizione delle policy coinvolge le business unit: ancora troppo pochi, anche se è un bel miglioramento rispetto al 16% del 2014.

Trend Micro acquisisce HP TippingPoint

L'azienda giapponese acquisisce uno dei fiori all'occhiello della sicurezza HP, portando nel proprio paniere d'offerta le funzionalità IPS e Firewall della famiglia TippingPoint, inclusi i DVlabs e la Zero Day Initiative

È stata annunciata oggi l'acquisizione da parte di Trend Micro di HP TippingPoint, la componente di soluzioni di sicurezza di HP che comprende le soluzioni Next Generation firewall e IPS, già in precedenza frutto di un'acquisizione da parte di HP.

Dal 2014 Trend Micro e TippingPoint hanno una partnership strategica e fonti ufficiali confermano che le due aziende continueranno a essere forti alleati dopo la transazione per lavorare ad attività OEM, per la sicurezza delle app e dei dati. L'arrivo nel paniere d'offerta delle soluzioni Firewall e IPS di nuova generazione rafforza ulteriormente le capacità di individuazione delle vulnerabilità e di protezione di rete dell'azienda giapponese in un contesto enterprise.

L'accordo, del valore approssimativo di 300 milioni di dollari, porterà alla creazione di una Network Defense business unit che avrà il compito di gestire più di 3.500 clienti enterprise.

«Le imprese hanno bisogno di una difesa dalle minacce che agisca su più livelli - ha commentato Eva Chen, CEO di Trend Micro - in grado di operare senza soluzione di

continuità attraverso tutta la struttura enterprise per occuparsi delle minacce prima, durante e dopo un attacco. Combinando il nostro sistema di rilevamento delle violazioni con le funzionalità di intrusion prevention e capacità di risposta delle soluzioni TippingPoint, questa nuova soluzione di prossima generazione per la difesa della rete rappresenta il complemento ideale della nostra protezione leader di mercato per data center ed endpoint».

L'apporto delle nuove soluzioni Firewall e IPS permetterà a Trend Micro di estendere la propria difesa multilivello rafforzando ulteriormente la capacità di rilevamento e prevenzione delle minacce.

L'acquisizione porta in dote anche competenze molto avanzate, inclusi i TippingPoint Digital Vaccine LABS

(DVLABS) specializzati nella realizzazione di filtri intelligenti capaci di fronteggiare vulnerabilità e bloccare attacchi "zero day" e anche la Zero Day Initiative indirizzata al rilevamento dei nuovi attacchi. Tutto ciò sarà integrato all'interno dell'infrastruttura di protezione Trend Micro Smart Protection Network che si pone alla base delle soluzioni dell'azienda giapponese.



Eva Chen, CEO di Trend Micro

BT protegge i dati del settore finanziario con il servizio di Ethical Hacking

di Riccardo Florio

BT adotta i test di sicurezza certificati STAR di CREST per proteggere le organizzazioni finanziarie dalle crescenti minacce informatiche

I dati di ricerche recenti mostrano come gli attacchi ai sistemi finanziari mondiali siano in continua crescita. I danni che possono derivarne in caso di successo sono potenzialmente enormi e tali da minare la fiducia degli investitori e dei correntisti. Il problema è che non sempre un istituto finanziario è in grado di valutare quanto il proprio sistema di sicurezza e prevenzione sia efficace. Un rimedio ha deciso di proporlo BT, con il lancio a livello globale di "BT Assure Ethical Hacking for Finance", un nuovo servizio di sicurezza che ha ideato per testare l'esposizione agli attacchi informatici delle organizzazioni che offrono servizi finanziari.

La ricchezza di dati personali sensibili e di valore in mano alle organizzazioni finanziarie, quali banche retail, banche d'investimento e società assicurative, le rende uno dei bersagli naturali più appetibili per gli hacker e i criminali informatici. Questo rischio, come evidenziato,

si è intensificato negli ultimi anni con il trasferimento online di un numero sempre maggiore di servizi finanziari per il cliente finale e l'aumento del trading elettronico. Assure Ethical Hacking for Finance, ha spiegato BT, si basa su metodologie evolute che simulano quelle dei cosiddetti "black hats" ossia gli hacker malintenzionati, per fornire una serie di test diretti ai vari punti di accesso ai sistemi IT di una banca così come ai "punti deboli" di un'organizzazione.



Questi includono phishing, dispositivi mobili e dispositivi hardware, dai Pc portatili alle stampanti, reti interne ed esterne, database e sistemi ERP complessi. Nell'ambito di queste aree e sistemi, BT testa e verifica i sistemi che possono accedere alla rete, ma effettua anche dei controlli per il rischio di errori umani, utilizzando ad esempio il "social engineering" per verificare il modo in cui i dipendenti applicano le policy in vigore.

È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**

In oltre 250 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business.

Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



**edizione
2015**



Sono disponibili anche
CLOUD COMPUTING E IT AS A SERVICE
STORAGE

Il libro è acquistabile al prezzo di 50 euro (più IVA 21%) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444