

CYBER LAW

AUMENTANO GLI ATTACCHI INFORMATICI IN ITALIA SECONDO IL RAPPORTO OAI

Più numerosi e più sofisticati gli attacchi che hanno interessato il nostro Paese nel 2014, secondo i dati appena pubblicati del Rapporto OAI, l'Osservatorio Attacchi Informatici, che indicano una crescita del 7,2% degli attacchi rilevati. Tra i risultati più significativi la conferma ai primi quattro posti di malware, social engineering, DoS e DDoS e furto dei dispositivi mobili, quali tipologie di attacco adottate. Tranne il furto dei device, tutte le altre

metodologie di attacco hanno registrato un aumento rispetto al 2013, con l'incremento maggiore relativo al malware e agli attacchi APT o attacchi mirati. Dati congruenti con quelli del Cnaipic (la Polizia Postale). Giunto alla quinta edizione il rapporto è realizzato da Malabo Srl con il patrocinio di AICA e Aipsi e con la sponsorizzazione di Business-e, HP, Risko, Gruppo Sernet, Technology Estate e Trend Micro. **pag.08-11**

CYBER LAW

MOBILE DEVICE RULES

Riccardo Abati, che si definisce "tecnocavvocato", affronta la questione dell'utilizzo dei mobile device in azienda da un punto di vista legale. In questi casi il profilo "normativo interno" diventa indispensabile per la predisposizione di una procedura che regoli la materia e crei i presupposti legali per incanalare la condotta del personale sia per quanto riguarda l'utilizzo di device aziendali sia personali (BYOD). **pag.15**

COMPLIANCE

SICUREZZA A 360° AL SECURITY SUMMIT 2015

Il 10 e 11 Giugno farà tappa a Roma il Security Summit, l'evento organizzato da Clusit e da Astrea, dedicato ai professionisti e appassionati del settore. Il punto forte del Security Summit sarà come sempre il livello dei contenuti, la competenza di docenti e relatori e la presentazione di tanti case study. Previste Tavole Rotonde, Sessioni Formative, Seminari e Atelier Tecnologici. **pag.18-21**

IN QUESTO NUMERO:

pag.3 EDITORIALE

• *Errare è umano. Perseverare è diabolico?*

NEWS

pag.5

- F5 presenta il servizio Web Application Firewall Cloud-Based
- Kaspersky Lab lancia la nuova versione di Small Office Security **pag. 7**
- Le soluzioni di G Data che proteggono il business
- Da tre a sei mesi per identificare le minacce avanzate

CYBER ATTACK

pag.08-11

• *Aumentano gli attacchi informatici in Italia secondo il rapporto OAI*

pag. 12-13

• *Security: attacchi cybercrime più facili e meno costosi*

CYBER LAW

pag.15

• *Mobile device rules*

CLOUD SECURITY

pag. 16-17

• *Cloud services: dalle linee guida del Garante al Digital Single Market*

COMPLIANCE

pag.18-21

• *Sicurezza a 360° al Security Summit 2015*

SOLUZIONI

pag.23

• *Check Point protegge i sistemi di controllo industriale*

pag.24

• *Cambiare approccio per proteggersi dagli attacchi mirati*



ROMA 2015
10 - 11 giugno
orario 9:00 - 18:00

SHERATON PARCO DE' MEDICI ROME HOTEL
Viale Salvatore Rebecchini, 39
Building N. 1

Ingresso gratuito

Security Summit è l'evento dedicato alla sicurezza delle informazioni che, da anni, coinvolge i partecipanti con contenuti e approfondimenti sull'evoluzione tecnologica del mercato, offrendo una molteplicità di stimoli, dibattiti e riflessioni.

Organizzato da



www.securitysummit.it

Errare è umano. Perseverare è diabolico?



di Gaetano Di Blasio

Il rapporto OAI (Osservatorio Attacchi Informatici), che negli anni ha visto crescere il numero di rispondenti/compileri del questionario, acquisendo sempre più valenza, seppur qualitativa, traccia uno scenario sempre più preciso della realtà italiana relativamente alla sicurezza informatica delle imprese.

Emerge una conferma: l'anello debole dei sistemi di sicurezza è il fattore umano. Alla base di un attacco andato a buon fine c'è sempre un errore, può trattarsi di un comportamento ingenuo, di una disattenzione, ma è comunque un errore.

Conosciamo tutti il detto latino "Errare humanum est, perseverare autem diabolicum", pur con le differenze dovute all'approssimazione tipica del tramandare orale. L'invito è a migliorare dai propri errori, evitando di ripeterli, ma qui non ci siamo! Non si può cercare una giustificazione, neanche minima.

Cominciamo a far riferimento al precedente aforisma di Cicerone: "Cuiusvis hominis est errare: nullius nisi insipientis, in errore perseverare", cioè "è cosa comune l'errare; è solo dell'ignorante perseverare nell'errore".

Molti dei problemi rilevati nel rapporto OAI sono di ordine organizzativo, quindi non si tratta di un "errore", ma si tratta di impostare delle politiche aziendali e di diffondere fino in fondo una cultura della sicurezza. Oggi esistono strumenti ludici che consentono di attuare formazione di buon livello. Così come ci sono strumenti che attuano automatismi per costringere il dipendente quantomeno a riflettere prima di compiere un'azione potenzialmente pericolosa per la sicurezza aziendale.

Sempre nella rubrica Cyber Attack, segnaliamo anche il Threat Report di Websense, dove si evidenzia un altro problema legato alla carenza di figure professionali dedicate alla sicurezza. Da questo punto di vista, mi dà un po' di conforto aver visto tanti studenti universitari al Security Summit di Milano.

Su questo numero, infine, ritroviamo la rubrica Cyber Law, cui si è aggiunta una nuova rubrica legata specificamente alla sicurezza del Cloud, a cura di CSA Italy, il Capitolo italiano della Cloud Security Alliance.

Numero 28
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



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

F5 presenta il servizio Web Application Firewall Cloud-Based

Giuseppe Saccardi

F5 Networks ha rilasciato un nuovo servizio gestito e fornito in modalità cloud per proteggere le applicazioni web dagli attacchi e garantire la conformità negli ambienti cloud e data center. Annunciato in occasione della conferenza Agility 2015, il servizio Silverline Web Application Firewall, ha chiarito la società, fornisce ai provider la possibilità di implementare rapidamente web application firewall (WAF) e funzionalità per l'attuazione di policy unificate e scalabili.

Il servizio comprende anche il supporto h24 da parte degli esperti F5 specializzati nella sicurezza che sfruttano le risorse del Security Operations Center di F5. I principali vantaggi del nuovo servizio evidenziati da F5 sono:

- **Deployment più facile:** il nuovo servizio WAF si prefigge di proteggere le applicazioni capitalizzando sulle capacità di sicurezza di F5 per la protezione contro gli attacchi avanzati di livello 7 (come quelli basati sulla geolocalizzazione, DDoS, SQL injection, le minacce zero-day, le applicazioni AJAX, i payload JSON, quelli indicati nella OWASP Top Tena) attraverso un servizio basato sul cloud.
- **Riduzione dei costi operativi:** è il derivato della possibilità di ridurre le spese operative attraverso l'outsourcing della gestione delle policy e delle funzionalità di compliance affidandola alle risorse SOC specializzate di F5. Quest'approccio, evidenzia F5, aiuta a eliminare i falsi positivi, proteggendo le applicazioni e i dati dalle minacce note ed emergenti. Il monitoraggio proattivo integra anche un'intelligenza esterna per la protezione delle applicazioni dalle minacce IP.

... continua su **Tom's Hardware**

Kaspersky Lab lancia la nuova versione di Small Office Security

Giancarlo Calzetta

La sicurezza nei piccoli uffici sta diventando una questione sempre più importante. Molte piccole aziende, infatti, conservano contatti e documenti relativi a grandi società di cui sono fornitrici, ma spesso non riescono a evitare che questi dati vengano trafugati e successivamente usati come base per attaccare bersagli più interessanti.

Per questo la nuova versione di Kaspersky Small Office Security incorpora, oltre alle classiche contromisure per il contenimento delle infezioni informatiche, una serie di tecnologie mirate ad arginare le falle più comuni causate da infrastrutture obsolete ed errori (o cattive abitudini) propri di personale poco addestrato. Innanzitutto, la suite copre tutti i dispositivi dell'azienda: dallo smartphone al PC, passando per Mac, Android e iOS. Ovviamente, su iOS non tutte le funzioni saranno abilitate, ma le più importanti non mancano, come il controllo degli url visitati tramite un browser speciale. Passando, poi, ai moduli specifici, la prima delle tecnologie degne di nota è quella che protegge i computer dalla criptazione malevola tipica dei malware che poi chiedono dei soldi per restituire i file codificati.

Tramite un meccanismo di protezione cloud based, infatti, si può istruire il software a bloccare tutti gli eseguibili che non hanno l'ok dal sistema di reputazione online di Kaspersky, impedendo ai ransomware di essere eseguiti. Anche se un utente lancia per errore un malware criptante (molto difficili da identificare), questo non viene eseguito e i dati sul disco restano al sicuro ma accessibili.

... continua su **Tom's Hardware**

An IDC Conference

GOING DIP: DOCUMENT, INFORMATION & PROCESS MANAGEMENT PER L'IMPRESA DIGITALE

Roma, 10 Giugno

Intervenire sui processi documentali è ancora oggi uno degli imperativi di molte aziende e pubbliche amministrazioni. Se da una parte è un obbligo imposto dalle normative che regolano il **percorso di digitalizzazione** della PA, dall'altra secondo IDC rappresenta un'enorme opportunità per ottimizzare l'intero **workflow documentale** e la relativa **infrastruttura di stampa** in un'ottica di controllo dei costi ed efficienza operativa, alla luce anche delle nuove potenzialità legate alle tecnologie cloud e mobili.Cogliere realmente questa opportunità, e non limitarsi ad attuare passivamente quanto prescritto dai nuovi regolamenti, significherà contribuire a generare reale valore per la propria azienda.

Tags

Gestione documentale, Print management, Managed Print Services, Workflow management, Dematerializzazione, Archiviazione sostitutiva, Fatturazione elettronica, Firma elettronica e grafometrica, Security, Cloud, Mobile

Premium Sponsor



Main Sponsor



Debate Lunch



PER INFORMAZIONI

Nicoletta Puglisi, Senior Conference Manager, IDC Italia
npuglisi@idc.com · 02 28457317

http://www.idcitalia.com/ita_DIP2015

#IDCDIP15



Le soluzioni di G Data che proteggono il business

Paola Saccardi

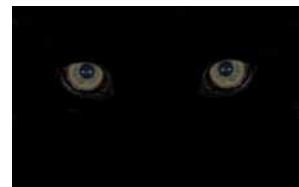


G Data, fornitore tedesco di sicurezza informatica, ha rilasciato una nuova gamma di soluzioni dedicate alla protezione delle aziende, che secondo il Rapporto Clusit stanno subendo danni molto elevati a seguito degli attacchi informatici. In particolare, G Data ha voluto mettere al sicuro tutta la rete estesa di terminali mobili che sempre più dipendenti utilizzano e che possono mettere a rischio la sicurezza dei dati e dei sistemi informativi aziendali. Grazie alla gestione estesa dei terminali mobili G Data mette al sicuro smartphone e tablet, non soltanto Android, ma anche iOS, che si possono integrare nella griglia di protezione centralizzata dell'infrastruttura IT aziendale. Le nuove soluzioni sono anche dotate di un sistema di controllo per evitare manipolazioni delle chiavette USB. Si tratta dello USB Keyboard Guard ed è gestibile tramite la console centralizzata e fornisce agli amministratori IT rapporti sulle tastiere o sulle chiavette USB autorizzate o bloccate. Le nuove soluzioni per le aziende comprendono G Data Antivirus Business, G Data Client Security Business, G Data Endpoint Protection Business, G Data Managed Endpoint Security. È possibile aggiungere il modulo supplementare per il backup centralizzato dei client e del mail gateway G Data MailSecurity. G Data Antivirus Business viene gestito attraverso la console centralizzata e protegge in modo automatico server e postazioni di lavoro, notebook e smartphone Android o iOS, senza impattarne le prestazioni.

... continua su **Tom's Hardware**

Da tre a sei mesi per identificare le minacce avanzate

Gaetano Di Blasio



Secondo le società di servizi finanziari e le aziende del retail, le minacce avanzate costituiscono il pericolo maggiore, anche perché non riescono a contrastarle con efficacia e, soprattutto con il dovuto tempismo.

Secondo una ricerca del Ponemon Institute, sponsorizzata da Arbor Networks, l'83% delle imprese nel finance e il 44% dei retailer registrano oltre 50 incidenti al mese, ma in media impiegano, rispettivamente, 98 e 197 giorni per identificarle.

Questo elevato "periodo di sedimentazione", sembra destinato a restare invariato, se non a peggiorare: infatti, il 58% delle società di servizi finanziari e il 71% dei retailer affermano di non essere ottimisti circa la propria capacità di migliorare tali parametri nell'anno a venire.

"Il tempo necessario a rilevare una minaccia avanzata è troppo lungo; gli attaccanti riescono a entrare e restare nascosti sufficientemente a lungo per causare danni irreparabili", commenta Larry Ponemon, chairman e fondatore del Ponemon Institute, che aggiunge: «Dalla nostra ricerca emerge la necessità di investire di più nella sicurezza a livello sia di personale sia di strumenti affinché le aziende possano rilevare e affrontare gli incidenti in modo più preciso ed efficiente». Aggiunge inoltre Matthew Moynahan, presidente di Arbor Networks: «È arrivato il momento di trovare un miglior equilibrio tra soluzioni tecnologiche, usabilità, workflow e le persone che le devono usare».

... continua su **Tom's Hardware**

Aumentano gli attacchi informatici in Italia secondo il rapporto OAI

di Gaetano Di Blasio

Malware, DDoS, social engineering e furto dei mobile device le principali cause, come confermano i dati della Polizia Postale. La crescita maggiore dovuta alla diffusione di ransomware. Molti gli attacchi non rilevati

Più numerosi e più sofisticati gli attacchi che hanno interessato il Nostro Paese nel 2014, secondo i dati appena pubblicati del Rapporto OAI (Osservatorio Attacchi Informatici): +7,2% gli attacchi rilevati. Tra i risultati più significativi la conferma ai primi quattro posti di malware, social engineering, DoS e DDoS e furto dei dispositivi mobili, quali tipologie di attacco adottate.

Tranne il furto dei device, tutte le altre metodologie di attacco hanno registrato un aumento rispetto al 2013, con l'incremento maggiore relativo al malware e agli attacchi APT (Advanced Persisted Threats) o attacchi mirati (Targeted attack). Dati congruenti con quelli del Cnaipic (la Polizia Postale).

Il pregio del rapporto OAI (Osservatorio Attacchi Informatici) consiste nel fatto che si focalizza esclusivamente sugli attacchi avvenuti in Italia, basandosi sull'elaborazione delle risposte raccolte attraverso un questionario online, che quest'anno, per avere un dato preciso da gennaio a dicembre 2014, è stato presentato nel periodo da gennaio a marzo 2015.

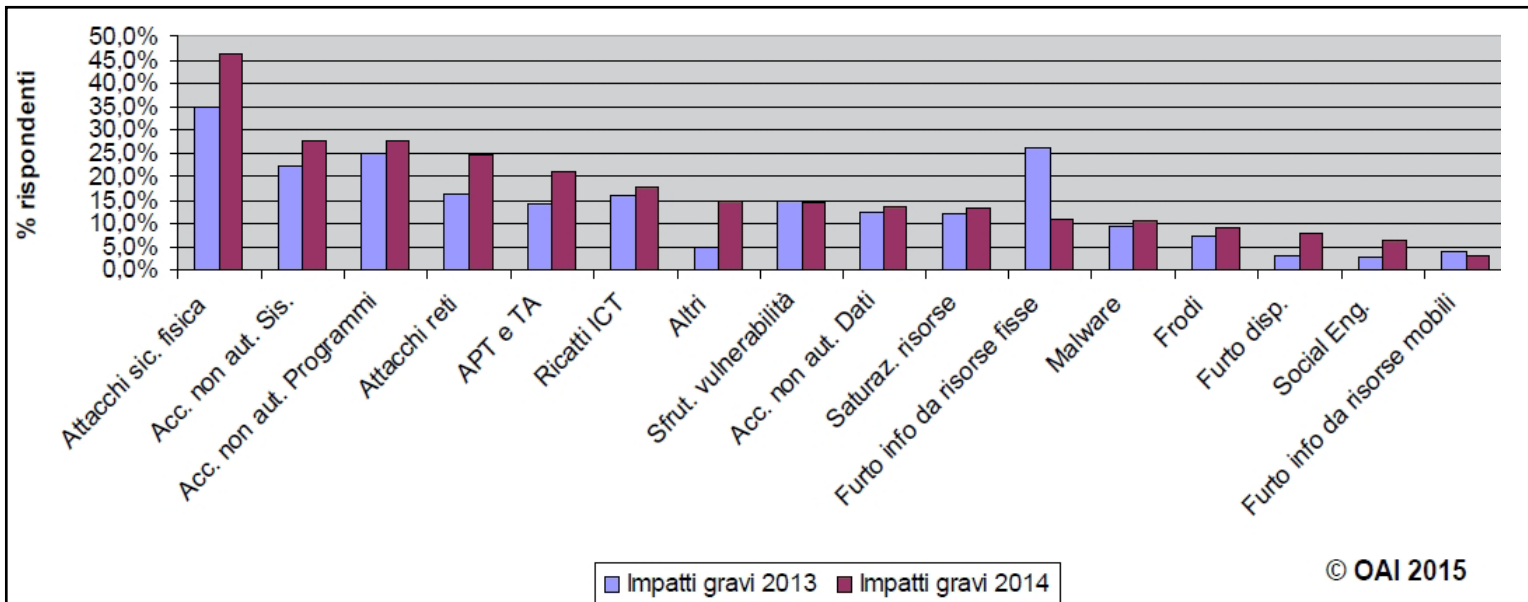
Giunto alla quinta edizione (ma una prima versione in forma di libro risale al 2005), il rapporto è realizzato

da Malabo Srl con il patrocinio di AICA (Associazione Italiana Calcolo Automatico) e Aipsi (Associazione Italiana Professioni della Sicurezza Informatica, capitolo italiano dell'ISSA, Information Systems Security Association) e con la sponsorizzazione di Business-e, HP, Riesko, Gruppo Sernet, Technology Estate e Trend Micro.

Ideatore e co-autore del rapporto, Marco Bozzetti, fondatore e Ceo di Malabo, oltre che membro del consiglio direttivo di Aipsi, tiene a precisare che l'analisi è di tipo qualitativo, in quanto il campione non è selezionato in base a requisiti di rappresentatività, ma prevede una compilazione spontanea, che è stata effettuata da 424 rispondenti (in crescita rispetto lo scorso anno). Le aziende che hanno partecipato appartengono a diversi settori economici, Pubblica Amministrazione, sia locale sia centrale, inclusa.

Da un punto di vista statistico, anche le comparazioni anno su anno non sono rigorose, perché il campione varia, ma si ottengono comunque dati di tendenza significativi e informazioni basilari anche per la sensibilizzazione sulla sicurezza informatica oltre che come riferimento per l'analisi dei rischi.

Impatti gravi per tipologia di attacco



Peraltro, lo sforzo dell'autore nel confrontare i dati con quelli disponibili da altre fonti, fornisce un quadro qualitativamente molto significativo. Va anche precisato che il questionario è piuttosto accurato, permettendo di raccogliere dati che è normalmente difficile ottenere.

Come accennato, il numero di attacchi è aumentato, soprattutto si è ridotta la percentuale di aziende che non ha rilevato alcun attacco. Bozzetti, inoltre, evidenzia un dato essenzialmente costante negli anni: mediamente le aziende che rilevano attacchi sono il 40% circa. Questo anche se i campioni di rispondenti sono diversi.

Secondo gli esperti si tratta di un valore troppo basso e questo indica che «molti attacchi non sono stati rilevati», evidenzia l'autore aggiungendo: «D'altro canto in Italia ci sono poche grandi aziende (circa 3600 quelle con più di 250 dipendenti, secondo l'Istat) e numerose piccolissime imprese, che non sono un obiettivo interessante per i cyber criminali».

Tale ipotesi sarebbe confermata dall'analisi degli attacchi nel 2014 per dimensione di azienda/ente dei rispondenti, in cui si evince le piccole imprese sono

quelle tra cui è più alta la percentuale di coloro che non hanno registrato violazioni alla sicurezza, mentre tra le grandi risulta più alta la percentuale di chi ha subito oltre 10 attacchi.

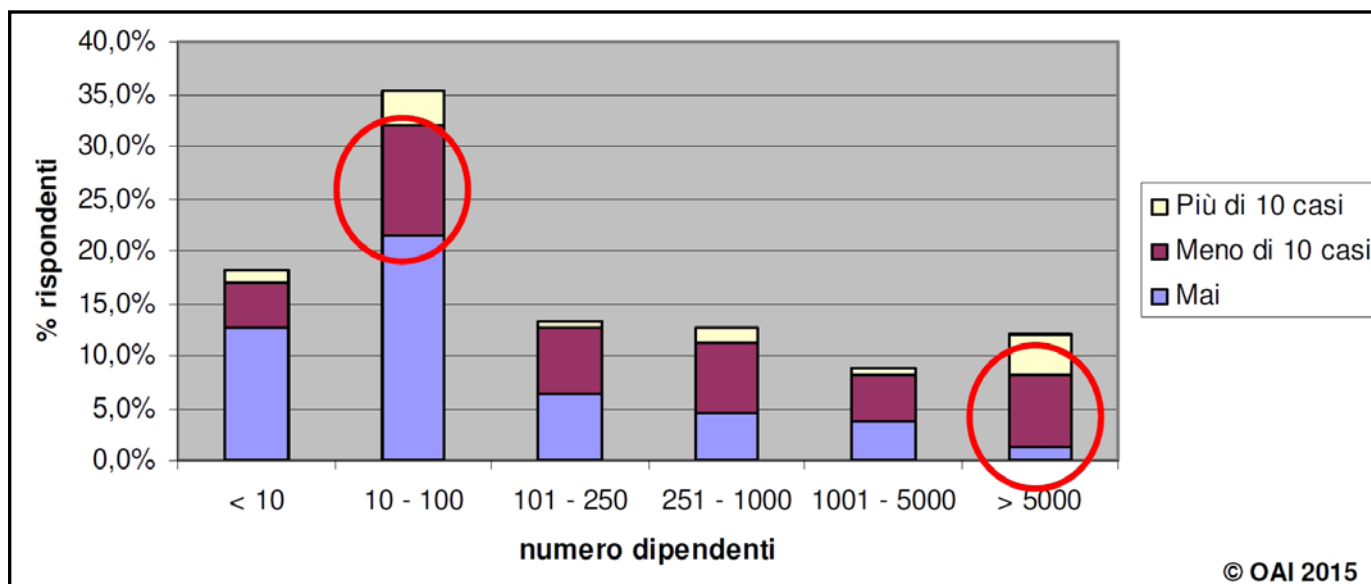
A livello mondiale, comunque, si stima che mediamente le aziende non rilevano circa i due terzi degli attacchi a loro rivolti

Altri dati interessanti riguardano l'analisi del rischio, che viene sempre più utilizzata come strumento decisionale a supporto delle strategie per la sicurezza. Altrettanto importanti sono le reazioni agli attacchi, che cominciano a prendere una certa consistenza, spaziando dalle azioni legali alle indagini interne ed esterne, per continuare con una serie di interventi tecnici.

Vulnerabilità e comportamenti scorretti emergono nell'analisi OAI 2015

Dal rapporto emerge che alla base di ogni attacco c'è lo sfruttamento di una o più vulnerabilità. Può essere tecnica, organizzativa o relativa alle persone, sia il comportamento scorretto o ingenuo di un utente finale, sia l'errore di un addetto ai sistemi informatici. Secondo i dati rilevati, l'anello più debole della catena

Attacchi nel 2014 per dimensione di azienda



È proprio il fattore umano e, non a caso, le principali criticità derivano da problemi organizzativi o da comportamenti dei dipendenti che permettono l'esecuzione dell'attacco.

In particolare, disattenzione e ingenuità si accompagnano alla scarsa conoscenza degli strumenti e alla mancanza di sensibilità sulla sicurezza informatica. Criticità amplificate dall'utilizzo di social network, email e dispositivi Usb. Tutti fattori che facilitano il furto d'identità da parte del cyber crime.

Quest'ultima è una delle tecniche più utilizzate negli attacchi mirati (APT), spesso attuata con lo spear phishing. Lo dimostrano diverse ricerche internazionali, che indicano il 2014 come l'anno dei "data breach".

Aumentano comunque i problemi dovuti alle vulnerabilità tecniche, non solo quelle nuove, che pure crescono con la complessità di tecnologie innovative nate con la virtualizzazione, il cloud e i sempre più potenti dispositivi mobili.

Spesso le vulnerabilità non sono scoperte per tempo dai fornitori e rimangono relativamente a lungo sfruttabili. Ma anche dopo la pubblicazione di una patch

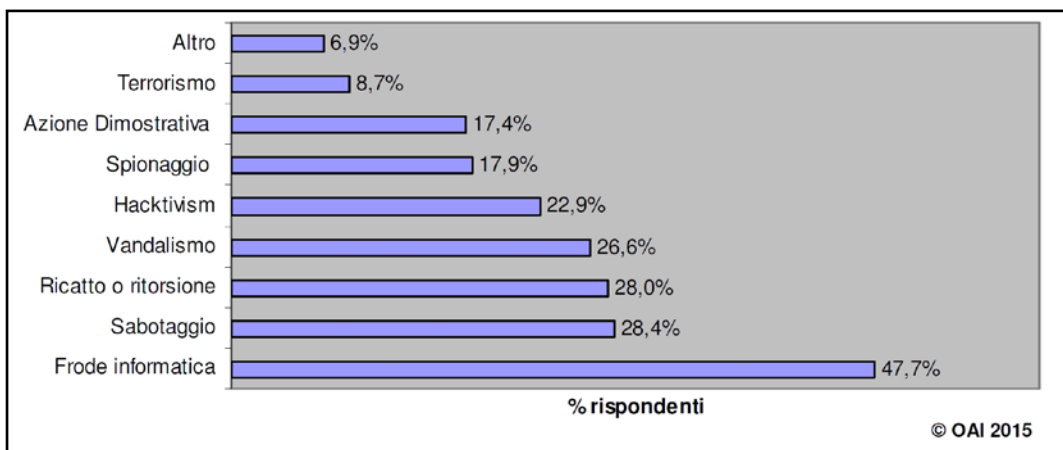
rimangono una spina nel fianco delle imprese, che non sempre riescono ad applicare gli aggiornamenti. Ciò è dovuto, purtroppo, soprattutto per problemi organizzativi: la non conoscenza delle disponibilità di patch, la mancanza di procedure per i test del software, il non rinnovo dei contratti di manutenzione del software, causato in molte realtà dal perdurare della crisi economica.

Impatti contenuti: solo il 13% quelli gravi

L'impatto registrato dalla maggior parte degli attacchi è stato ridotto, tanto è vero che nel 68,4% il ripristino è stato realizzato in giornata, ma nel 4,1% dei casi è stato necessario addirittura un mese. In ogni caso, gli attacchi considerati gravi (la valutazione è stata lasciata ai rispondenti) sono stati una percentuale ridotta (circa il 13%).

Più interessante osservare la gravità dell'attacco in funzione al tipo di attacco subito: al primo posto si trova la sicurezza fisica e questo, per certi versi conferma la scarsa considerazione verso la information security in Italia. Seguono gli accessi non autorizzati ai sistemi

Motivazioni per attacchi futuri



ICT e alle loro applicazioni, gli attacchi alle reti e gli attacchi APT.

Va però osservato che gli attacchi mirati, laddove l'impatto è stato considerato grave, sono, dopo le violazioni alla network security, quelli che hanno registrato il maggior incremento rispetto al 2013.

Gli attacchi ATP sono, di fatto, più una metodologia che un vero e proprio tipo di attacco. Essi si basano su più fasi e utilizzano più tecniche. È evidente che sono tra i più costosi da realizzare e, pertanto sono utilizzati appunto per attacchi mirati in genere verso obiettivi "ricchi". Non stupisce che siano tra le prime posizioni tra gli attacchi gravi, mentre preoccupa la loro crescita anche in Italia. Tra il 2013 e il 2014 sono il tipo di attacco più aumentato dopo il ramsonware, che l'anno scorso ha visto un boom ovunque nel mondo.

Sistemi aggiornati

Tra gli aspetti positivi registrati dal rapporto OAI 2015 c'è una confortante fotografia dei sistemi informativi, per la maggior parte tecnicamente aggiornati, con una parte del campione significativa che dispone di architetture ad alta affidabilità (circa il 50%). Pure importante è che il 34% del campione disponga di un piano per la business continuity.

Altre caratteristiche del campione sono l'utilizzo del cloud da parte il 50% dei rispondenti, quello delle VPN dal 63,6%. Quasi il 66% ricorre all'outsourcing,

almeno in parte. Inoltre, il 23,4% non consente il

BYOD (Bring Your Own Device), perché pone problemi alla sicurezza.

Pure positivo il fatto che quasi il 70% dei rispondenti ha definito, pubblicato e gestisce le "policy" sulla sicurezza e le relative procedure organizzative, di riferimento anche per i suoi fornitori, mentre per il 15% sono in corso di definizione.

D'altro canto, resta l'interrogativo sulla rappresentatività di tale campione: la realtà italiana nel suo complesso come si pone rispetto all'alta affidabilità e alla business continuity?

Paura per il futuro

Infine, il rapporto ha ottenuto un quadro di quello che si aspettano le imprese per il prossimo futuro in termini di attacchi temuti e perché. In particolare, le frodi informatiche sono considerata la principale motivazione per gli attacchi futuri, ma, contemporaneamente, sono anche il tipo di attacco meno temuto (preoccupa solo il 13% dei rispondenti). Mentre fanno più paura il social engineering e il furto dei dati dai dispositivi mobili, probabilmente perché sono stati sperimentati quali gli attacchi con gli impatti maggiori.

La paura di un attacco mirato è indirettamente confermata dal 28,4% di rispondenti che considerano il sabotaggio come una delle più probabili ragioni di attacco.

Security: attacchi cybercrime più facili e meno costosi

di Gaetano Di Blasio

Il Threat Report 2015 dei Websense Security Labs rivela nuove tecniche di elusione che riducono l'efficacia delle sandbox. Calano i prezzi del Malware as a Service.

Il Threat Report 2015 dei Websense Security Labs si basa sui dati raccolti dal ThreatSeeker Intelligence Cloud, in grado di ricevere oltre cinque miliardi di input al giorno da 900 milioni di endpoint in tutto il mondo. Da quest'anno, però, sono state aggiunte altre fonti, frutto del lavoro di cooperazione tra diversi protagonisti della sicurezza, impegnati a contrastare le ingenti risorse di ricerca e sviluppo impiegate dalle organizzazioni cybercriminali.

L'interpretazione degli esperti dei Websense Security Labs, poi, si basa su interviste e indagini eseguite da ricercatori e ingegneri in Europa, Medio Oriente, Asia e Nord America. Emiliano Massa, Director of Regional Sales Websense South EMEA (una region recentemente allargatasi comprendendo Francia e Israele), evidenzia una tendenza in particolare: effettuare attacchi diventa sempre più facile, grazie all'evoluzione dei servizi di cybercrime.

In sostanza, si assiste alla crescita di un mercato, che risponde a tutte le logiche standard del business: aumenta la concorrenza e conseguentemente scendono i prezzi e vengono sviluppati nuovi servizi, più performanti e user friendly. Il risultato è un incremento di funzionalità all'avanguardia che agevolano i criminali nel loro intento. Per esempio catene di redirect, riutilizzo di codice e altre tecniche, che consentono tra l'altro a queste persone di rimanere anonime, rendendo l'attribuzione sempre più

lunga e inaffidabile.

Addirittura, afferma Massa, spesso non conviene neanche spendere tempo e risorse

in attività forensi che non portano né a identificare l'origine dell'attacco né a comprendere come intervenire per evitare che si possa ripetere. Del resto, viene evidenziato nel rapporto, è diventato più difficile fare una corretta attribuzione di un attacco informatico, data la facilità con cui gli attaccanti possono falsificare le informazioni, aggirare la registrazione e il monitoraggio o comunque rimanere anonimi. Spesso un'analisi delle stesse prove circostanziali può portare a conclusioni molto diverse. Per questo in Websense hanno sviluppato, con il rilascio di Triton APX all'inizio dell'anno, le soluzioni DTP (Data Threat Prevention), che si basano sull'analisi delle anomalie osservate sulla rete, per esempio in termini di comportamenti non consueti per un utente o non congruenti al contesto. Come il caso di un utente che risulta loggato contemporaneamente da due IP diversi.

Il Threat Report 2015 dei Websense Security Labs spiega quali sono le tendenze comportamentali e tecniche del cybercrime e allo stesso tempo fornisce informazioni e suggerimenti utili per aiutare i professionisti della sicurezza a pianificare la loro strategia di difesa della rete.



Emiliano Massa - Websense



Luca Mariani
Websense

Ecco altri tra gli aspetti principali emersi dallo studio. Innanzitutto, come accennato il cybercrime è più facile, anche per persone alle prime armi, accedendo più facilmente ed economicamente a exploit kit in affitto attraverso servizi Maas (Malware as a Service), così come all'acquisto o noleggio di porzioni o di un intero attacco informatico complesso e pluri strutturato. Infatti, si è affinata ulteriormente la capacità di abbinare tecniche nuove e tradizionali, dando origine a soluzioni maligne altamente evasive.

Sembra che gli autori degli attacchi si stiano concentrando più sulla qualità, piuttosto che sulla quantità come in passato. Peraltro, si parla di Digital darwinismo, facendo riferimento alla sopravvivenza delle minacce in grado di evolvere. Non solo: si assiste al riutilizzo di vecchie minacce, per esempio i macro virus. Nello specifico, Luca Mairani, senior sales engineer di Websense, riporta di un recente attacco indirizzato in Italia, che partiva con mail plausibili con in allegato un file Word, il quale attivava una macro per scaricare malware, soprattutto Cryptolocker.

Se le minacce sono diminuite (i Websense Security Labs hanno osservato 3.9 milioni di minacce alla sicurezza nel 2014, il 5,1% in meno rispetto al 2013), sono però sempre più sofisticate, aumentando quelle utilizzate in attacchi con logiche multifase tipo APT. Qui, sottolinea Mairani, le criticità sono legate soprattutto a Java e altri sistemi, come Acrobat Adobe o Microsoft Explorer, ma anche open source, che le aziende devono mantenere nella vecchia versione perché è la sola compatibile con le applicazioni legacy aziendali. Quindi non possono applicare le patch e rimangono esposti a vecchie e nuove vulnerabilità.

A rendere più sofisticati gli attacchi APT concorre anche il fatto che i cyber criminali hanno reinventato la metodologia

di attacchi per ridurre la visibilità delle minacce. Lo hanno fatto seguendo in maniera sempre meno lineare la tradizionale catena di attacco. Gli attacchi sono più difficili da rilevare se alcuni stadi vengono saltati, ripetuti o applicati solo parzialmente, riducendo così la visibilità della minaccia stessa. Un'attività varia fortemente se svolta in una diversa fase della catena di attacco. Così come l'attività di spam si concentra sulle prime fasi della catena, altre fasi della catena subiscono diverse attività malevole. Alcune fasi hanno visto un maggior numero di attività; altre ne hanno rilevate molto meno rispetto all'anno precedente.

Per concludere, va evidenziata ancora una volta la carenza di professionisti della sicurezza: ne mancano 2 milioni, secondo il rapporto e il problema, aggiunge Massa, è che la formazione di una figura altamente qualificata sulla cybersecurity richiede almeno 11 anni.

Ma il bisogno di aumentare l'IQ, cioè l'intelligenza sulla sicurezza non riguarda solo i professionisti, occorre continuare a insistere per educare i propri dipendenti e adottare strumenti automatici che impediscono ai dipendenti di commettere errori fatali o, peggio, atti dolosi intenzionali. Il rapporto continua a porre al primo posto le cosiddette minacce interne.

Due ultimi punti rilevati: la fragilità delle infrastrutture fragili, con un aumento delle minacce che si espandono nell'infrastruttura di rete stessa, per esempio vulnerabilità nascoste sono state rinvenute all'interno dei codici di base Bash, OpenSSL, SSLv3 e altri che sono stati in uso per decenni. Infine, l'Internet of Things (IoT) che avrà un impatto notevole sull'esposizione agli attacchi informatici, poiché si stima che la crescita di dispositivi connessi raggiungerà una cifra tra i 20 e i 50 miliardi entro il 2020.

Gaetano Di Blasio

IDC Mobiz – Mobility Forum 2015

Powering individual productivity and business agility

Bologna, 18 Giugno



Nel 2014, IDC ha evidenziato un'evoluzione delle aziende dalla fase passiva della consumerizzazione a quella attiva del mobile first, durante la quale la mobility da problema da gestire è diventata leva per rendere le organizzazioni più competitive dal punto di vista dell'efficienza e della produttività. Nel 2015, uno stadio di ulteriore maturità porterà le strategie di enterprise mobility a evolvere verso soluzioni e progetti per estendere l'interazione attraverso device e app mobili anche fuori dalle aziende, abbracciando partner e clienti. E' l'inizio di quella che IDC chiama la fase customer first and mobile first, dove il personale aziendale, la catena del valore e i clienti diventano parte di una strategia mobile complessiva che vedrà l'IT aziendale sempre più coinvolto e impegnato.

Tags

Enterprise mobility, Mobile security, Mobile device management (MDM), Mobile application management (MAM), Mobile enterprise application platform (MEAP), BYOD/CYOD, Mobile B2C services, Mobile enterprise app store, Social

Premium Sponsor



Main Sponsor



Debate Lunch



PER INFORMAZIONI

Nicoletta Puglisi, Senior Conference Manager, IDC Italia
npuglisi@idc.com · 02 28457317

http://www.idcitalia.com/ita_Mobiz2015

#IDCMobiz15



MOBILE DEVICE RULES

di Riccardo Abeti

Come affrontare l'utilizzo dei dispositivi mobili in ambito aziendale dal punto di vista legale

Internet, per come lo si conosceva nello scorso ventennio è, oggi, profondamente mutato con la diffusione esponenziale di strumenti come il cloud ma anche con la progressiva miniaturizzazione di potenti device, gli smartphone, che, oggi, rappresentano una parte importante dei punti di accesso alla Rete. Il mondo aziendale, volente o nolente, è caratterizzato dall'esigenza di diffondere le informazioni a tutti i soggetti che ne abbiano necessità e farlo in modo tempestivo, al contempo occorre regolamentare l'uso dei device da parte del personale. Sempre più aziende avviano progetti di Mobile Enterprise Management. La sensibilità a questo tema è in costante crescita, anche se talvolta se ne trascura la portata affrontando il problema in modo settoriale e non olistico.

Se la gestione dei "mobile device" è per lo più entrata nella prassi delle grandi aziende, quelle medio piccole continuano ad ignorarne risvolti, ricadute, implicazioni. Una forte leva che ha spinto il fenomeno del "mobile" è costituita dalla trasformazione del mercato del lavoro segnata dall'avvento del telelavoro e del c.d. smart working. Oggi, lavorare in mobilità è non solo un'esigenza ma, soprattutto, un dato di fatto. La necessità di uno spazio fisico, gli orari di lavoro e gli stessi strumenti di lavoro devono essere ripensati. I profili giuridici di questo fenomeno vanno dalla trasversalità rispetto alle diverse tipologie di contratti di lavoro, all'esigenza "normativa interna" degli enti che intendono regolare la materia, siano essi aziende o pubbliche amministrazioni. A proposito del profilo "normativo interno", infatti, si rende indispensabile la predisposizione di una procedura che regoli la materia e crei i presupposti legali per incanalare la condotta del personale sia in relazione all'uso di device aziendali che in relazione all'uso di device personali nell'ambi-



Riccardo Abeti ama definirsi "tecno-avvocato" in quanto esperto di leggi relative all'Information e Communication Technology. Socio di EXPLegal, da oltre 15 anni si confronta con tecnici e top manager per risolvere problemi legati al rispetto delle leggi e alla sicurezza IT

to dell'attività aziendale (c.d. BYOD). Nel caso ci si riferisca a device personali, il caso del BYOD, le implicazioni e difficoltà di controllo (inteso nella sua accezione lecita ovviamente), si presentano sotto diversi aspetti che vanno dalla conduzione delle attività aziendali su dispositivo mobile, fino alla messa in sicurezza di un supporto che, pur non appartenendo all'azienda, elabora documenti e file di interesse aziendale.

Al di là delle soluzioni tecnologiche di questo fenomeno, peraltro ampiamente esplorate nel documento della Oracle Community for Security intitolato "Mobile enterprise", occorre tenere in considerazione aspetti di natura organizzativo-legale, si pensi alla possibilità, diffusa, che il controllo vada esteso oltre i lavoratori soggetti alla vigilanza del datore di lavoro; in quest'ottica si pensi ai fornitori, agli agenti, agli intermediari di qualsiasi tipo. Per guidare il controllo dell'uso che questi ultimi, ovvero i soggetti che sono più distanti dal perimetro di controllo del datore di lavoro/imprenditore, fanno del proprio dispositivo, si può ricorrere a diversi strumenti la cui capacità di condizionamento è gradatamente minore:

- il contratto che regola i reciproci rapporti,
- il codice etico di cui al d.lgs. 231 del 2001.

Naturalmente non bisogna sottovalutare la compenetrazione dell'ambito mobile con quello dei social media, che impone nella maggior parte dei casi una gestione congiunta delle problematiche. Infine, per valutare i profili elencati (e gli altri non nominati in questa sede), occorre partire da un'analisi di impatto che soppesi le implicazioni, in relazione al tipo di soggetto a cui si applica (ad esempio se privato o pubblico), al settore merceologico, alla struttura interna dell'azienda, alla forza del brand e alle modalità di lavoro adottate.

Cloud services: dalle linee guida del Garante al Digital Single Market

Le linee guida pubblicate dal Garante per la protezione dei dati personali sulla profilazione online dei dati degli utenti che navigano nel Web

*di Gloria Marcoccio e
Alberto Manfredi*

Il 6 Maggio 2015 l'Autorità italiana Garante per la protezione dei dati ha pubblicato le Linee guida in materia di trattamento di dati personali per profilazione online (Pubblicato lo stesso giorno sulla Gazzetta Ufficiale n. 103).

Le linee guida intendono chiarire ed indicare agli operatori stabiliti in Italia che offrono servizi della Società dell'Informazione (motori di ricerca, servizi cloud, servizi di pagamento on line, posta elettronica, social network, ..) apposite modalità per adempiere ai requisiti di legge privacy, essenzialmente Informativa e Consenso, nel contesto dei processi di profilazione on line (per finalità di marketing, per erogare uno specifico servizio, ..), sia nei riguardi degli utenti autenticati, cioè quelli che accedono ai servizi tramite un account, sia nei riguardi degli utenti che fanno uso dei servizi in assenza di autenticazione, come in caso di semplice navigazione online. Le modalità indicate dall'Autorità nelle sue linee guida comportano impatti anche di natura tecnica per la realizzazione e gestione dell'Informativa e del Consenso online (in funzione anche degli elementi identificatori utilizzati quali le credenziali di accesso, i device fingerprinting,... e contesti di profilazione quali i servizi di posta elettronica, incrocio di dati e relativo utilizzo per più finalità,...).

Le linee guida non hanno di per sè natura prescrittiva,

ma come espressione della interpretazione di legge prodotta dalla Autorità competente hanno un chiaro valore per cui occorre tenerle presenti qualora i servizi erogati contemplino processi di profilazione online di utenti, autenticati o meno.

La materia trattata è di ampio respiro e si presta certamente a diverse letture che, in funzione dei contesti tecnologici e soprattutto del business degli operatori interessati, possono far emergere nelle linee guida punti chiari ed altri decisamente meno.

Tra questi hanno una particolare valenza, sia da un punto di vista normativo che implementativo, quegli aspetti che devono necessariamente trovare un coordinamento operativo con il Provvedimento sui cookie (questo, diversamente dalle linee guida, è di natura prescrittiva con relative specifiche sanzioni in caso di inadempienze) che entrerà in vigore nei primi giorni di Giugno 2015. Il riferimento è a quanto la linea guida indica in termini di misure relativamente all'Informativa, Consenso ed esercizio dei diritti degli interessati riguardo all'uso delle tecniche di device fingerprinting (riconoscimento di un device, in modo non necessariamente univoco, in base a suoi determinati parametri che sono direttamente accessibili in lettura via internet) che possono essere utilizzate sia ai fini della profilazione per azioni di marketing basate sull'analisi del comportamento



online dell'utente, sia come supporto in processi di autenticazione&sicurezza on line (come ad esempio per alcuni servizi di mobile payment che sono legati anche all'identificazione del device).

Occorre poi ricordare che per alcuni tipi di profilazione è necessario effettuare la Notifica all'Autorità Garante per i dati personali (sono previste sanzioni in caso di inadempienza): in una linea guida dedicata alla profilazione on line sarebbe quantomeno utile avere un riferimento che ricordi questo importante adempimento.

Deve poi sempre essere tenuto presente che le linee guida si rivolgono agli operatori della società dell'informazione che sono stabiliti in Italia: in conseguenza di ciò l'implementazione del complesso delle misure indicate nella linea guida da parte di tali aziende, potrebbe comportare uno squilibrio con possibili ricadute sul business rispetto al quadro di way of working valido per le aziende non stabilite in Italia, che comunque offrono servizi on line, notoriamente worldwide.

Questa linea guida fa poi amplissimo, spesso letterale, riferimento alle prescrizioni che il Garante ha emesso nei riguardi di Google l'anno scorso tramite apposito provvedimento nel quale sono stati previsti consistenti tempi di adeguamento dimensionati sulla complessità di quanto richiesto e la molteplicità dei sistemi Google interessati (per questi adempimenti Google sta se-

guendo un apposito protocollo di verifica concertato con l'Autorità).

Proprio in relazione alle tempistiche di adeguamento ed al notevole complesso di ambiti e misure considerate, pur essendo ben consapevoli che tali linee guida non hanno natura prescrittiva ma sono certo autorevole e competente interpretazione della normativa, sarebbe auspicabile, e sarebbe certo una motivazione in più per procedere con implementazioni coerenti con essa, che l'Autorità valuti l'opportunità di pubblicare una Q&A di corredo e di indicare un grace period a favore di coloro che decideranno di allinearsi alla linea guida.

Un'ultima considerazione va rivolta alla recente pubblicazione della strategia sul mercato unico digitale europeo (Digital Single Market) da parte della presidenza della Comunità Europea (http://ec.europa.eu/priorities/digital-single-market/index_en.htm) che nell'ambito dei 3 pilastri fondanti pone molta enfasi sul sostegno allo sviluppo del mercato e-commerce tra i 28 stati membri, armonizzando e semplificando norme e procedure, e sullo sviluppo del Cloud Computing e Big Data, con grande attenzione alla cyber security e privacy.

Pertanto un corretto e prosperoso sviluppo del mercato dei servizi online, di cui la profilazione è una delle tematiche importanti, è ormai un obiettivo europeo e non più soltanto nazionale.

Sicurezza a 360° al Security Summit 2015

di Luca Bechelli

Il Sistema Pubblico di Identità Digitale (SPID), la sicurezza dei dati in ambito sanitario-ospedaliero e l'attività dei Cert in casi reali di attacchi informatici tra i temi di punta dell'edizione romana del Security Summit 2015

Il 10 e 11 Giugno farà tappa a Roma il Security Summit, l'evento organizzato da Clusit e da Astrea, tanto atteso dai professionisti e gli appassionati del settore. Il punto forte del Security Summit sarà come sempre il livello dei contenuti, la competenza di docenti e relatori e la presentazione di tanti case study. Durante i due giorni sono previste 4 Tavole Rotonde, 8 Sessioni Formative, 5 Seminari e 12 Atelier Tecnologici.

Si affronteranno i temi di maggior interesse del momento: cyber crime, cyber war, cyber attack e cyber defence, Intelligence. Si parlerà della sicurezza dei dati in ambito sanitario-ospedaliero e dell'attività dei Cert in casi reali di attacchi informatici. Altro tema super gettonato è quello della sicurezza dei dispositivi mobili, viste le opportunità offerte dalle tecnologie mobili che stanno cambiando il modo di lavorare delle persone. Ma si tratterà anche di: cloud security, sistemi Scada e infrastrutture critiche, competenze e certificazioni professionali, sicurezza dei data center, computer forensics e tanto altro. Ogni giornata sarà caratterizzata da una sessione plenaria di apertura. Il 10 sarà presentato il Rapporto Clusit 2015 sulla sicurezza ICT in Italia, frutto del lavoro di un centinaio di esperti e dovuto alla collaborazione di un gran numero di soggetti pubblici e privati, che hanno condiviso con Clusit informazioni e dati di prima mano e

condiviso le proprie esperienze sul campo. Tra i contributi più autorevoli dell'edizione 2015 del rapporto, anche quello della Polizia Postale e delle Comunicazioni e quello del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza, i cui vertici interverranno nella sessione di apertura.

La seconda giornata si aprirà invece con una tavola rotonda che intende fare il punto sul Sistema Pubblico per la gestione dell'Identità Digitale (SPID) e sugli aspetti di sicurezza, con la partecipazione di alcuni dei principali soggetti istituzionali coinvolti nel progetto, oltre a Identity Provider e Fornitori di Servizi.

A proposito di SPID, presentiamo un articolo di Luca Bechelli, membro del Direttivo e del Comitato Tecnico Scientifico del Clusit.

Il sistema pubblico per la gestione dell'Identità Digitale

Il Sistema Pubblico per la gestione dell'Identità Digitale (SPID), introdotto nel Codice dell'Amministrazione Digitale con il D.L. del 21 Giugno 2013, ha come obiettivo fornire al cittadino una piattaforma unica di accesso ai servizi erogati su internet dalle pubbliche amministrazioni, aperta alla partecipazione dei soggetti privati. Siamo ormai al debutto: sono attesi i pareri del Ga-



Foto di rito con il Rapporto Clusit 2015 al Security Summit di Milano

rante per la Privacy e la successiva firma del Direttore dell'AgID; dopo alcuni mesi di sperimentazione, l'aspettativa è quella di ottenere il rilascio di 3 milioni di identità digitali SPID entro la fine del 2015 .

L'identità digitale SPID consisterà in un account che ogni cittadino potrà ottenere da un "identity provider", un soggetto (pubblico o privato) accreditato presso AgID. A tale account potranno essere associati una serie di attributi identificativi (es: dati anagrafici), secondari (numero di telefoni, email, PEC, domicilio ...) e qualificati (qualifiche, abilitazioni professionali, poteri di rappresentanza). Questi ultimi, in particolare, saranno "collegati" all'identità SPID ma gestiti da ordini professionali, enti, associazioni, etc..., diversi dall'Identity Provider.

Con un solo account il cittadino potrà quindi accedere a tutte le applicazioni web di "fornitori di servizi", anch'essi accreditati presso AgID, allo stesso modo con cui oggi è possibile utilizzare un account Gmail o Facebook per l'autenticazione a servizi diversi, pratica sempre più diffusa in ambito cloud e social.

Rispetto a tali servizi tuttavia, l'identità digitale SPID

costituisce un decisivo passo avanti verso la c.d. "cittadinanza digitale": Identity Provider e Fornitori di Servizi sono tenuti al rispetto delle normative nazionali, in primo luogo quella per la tutela dei dati personali, ed ai

regolamenti emessi e periodicamente aggiornati da AgID, anche in relazione alle misure di sicurezza informatica. In tale contesto, anche il "cittadino digitale" non è un soggetto passivo, dato che le sue azioni sono "imputabili", manlevando i Fornitori di Servizi dalla responsabilità di sorveglianza delle attività sui propri siti (prevista dall'art. 17 del D.Lgs. 9 aprile 2003, n. 70).

Dal punto di vista della sicurezza, gli Identity Provider dovranno consentire l'accesso all'identità SPID mediante differenti meccanismi di autenticazione, a sicurezza crescente; i Fornitori di Servizi, dal canto loro, potranno decidere quale tra i meccanismi di autenticazione richiedere al cittadino sulla base di un'analisi dei rischi. La sicurezza diventa pertanto un fattore abilitante, adeguato alle effettive esigenze di protezione di servizi potenzialmente molto diversi: se lo SPID fosse solo concepito come una "soluzione per l'autenticazione sicura", rischierebbe di essere relegato a utilizzi particolari, mentre è obiettivo del Legislatore renderlo uno strumento di uso comune, destinato ad esempio anche ad applicazioni di semplice consultazione .



E' tutto oro quel che luccica?

Probabilmente no. SPID ha verosimilmente tutti i difetti fisiologici di un'iniziativa di grande prospettiva: si devono tenere in considerazione sia i rischi che SPID non riesca a offrire le necessarie garanzie di cittadinanza digitale, sia che per farlo non abbia le opportune caratteristiche di usabilità e attrattiva verso gli utenti finali, come in passato è avvenuto per iniziative analoghe al loro esordio (es: firma digitale, PEC).

Dal punto di vista della sicurezza informatica, secondo alcuni si corre il pericolo di concentrare nelle mani degli Identity Provider un patrimonio di "big data" potenzialmente pericoloso per la privacy degli utenti, tenuto conto che i soggetti che probabilmente avranno le caratteristiche per svolgere tale ruolo sono gli operatori Telco, le Banche ed altri attori che potrebbero già avere un notevole capitale di informazioni sui cittadini.

Per altri, SPID è percepito come una "targa" apposta su ogni utente delle autostrade digitali, per finalità di con-

trollo. In tal senso, si può osservare come i regolamenti tecnici (attualmente in bozza) non sempre rappresentano come centrali i fattori di rischio degli utenti rispetto agli Identity Provider ed ai Fornitori di Servizi, nella logica che la sicurezza della piattaforma coincida con la sicurezza del cittadino. Infine, non sembrano ancora essere previsti elementi di controllo dell'utilizzo delle identità digitali (es: sistemi di notifica in caso di

tentativi di accesso) a tutela dell'utente, di comprovata efficacia nell'ambito dei servizi bancari.

Tutti questi potenziali limiti (da rivalutare quando la piattaforma sarà definitivamente resa disponibile) devono però essere misurati in rapporto alla realtà corrente. Già oggi, come detto, i soliti "big" fornitori di servizi di posta, cloud e social, erogano servizi di autenticazione centralizzata utilizzati da milioni di utenti; servizi che sono solo apparentemente gratuiti, perché in cambio di gigabyte di spazio, o dell'opportunità di ritrovare i nostri vecchi compagni di scuola, registrano (loro sì!) big data di informazioni personali senza dover sottostare al rispetto delle normative nazionali. In tali ambiti si realizzano nel concreto i timori rivolti a SPID, con l'aggravante che, in assenza di normative adeguate (a livello europeo e nazionale sono in discussione diverse ipotesi di evoluzione), il Regolatore e le Forze dell'Ordine hanno su di essi una limitata capacità di azione.

Naturalmente non possiamo adottare una posizione tesa

al “male minore”, pertanto è opportuno che ai vari dubbi siano date risposte adeguate: a tale scopo, bisogna ricordare che SPID ha il vantaggio di essere stato disegnato tecnicamente su standard aperti, che AgID ha reso disponibili i regolamenti tecnici fino dalle prime bozze, e l’Ufficio del Garante per la Protezione dei Dati Personali dovrà esprimersi sulla bontà delle tutele e garanzie offerte. Alcuni dei limiti evidenziati potrebbero poi legittimamente essere ritenuti di secondaria importanza, e superati a regime, per colmare con urgenza un ambito ove la Pubblica Amministrazione ha un evidente ritardo. Il timore di coloro che credono che con l’identità SPID si venga “targati” sulla rete non devono però essere

sottovalutati, anche solo in termini di “percezione” dello strumento, perché tale percezione ne influenzerà la diffusione. In tal senso, SPID ha la grande opportunità di costituire un mezzo di notevole sensibilizzazione dei cittadini sulla sicurezza informatica.

Il cittadino dovrà essere reso consapevole di cosa significa e quali vantaggi determinano l’essere “cittadini digitali” piuttosto che semplici, apolidi, “naviganti”. SPID aprirà uno spazio di cittadinanza nel quale valgono le regole, che sono soprattutto una tutela delle persone. Uno spazio che non è diverso dalle strade in cui ci muoviamo con le nostre automobili, dove i limiti di velocità non servono a generare multe, ma a salvaguardare se stessi e

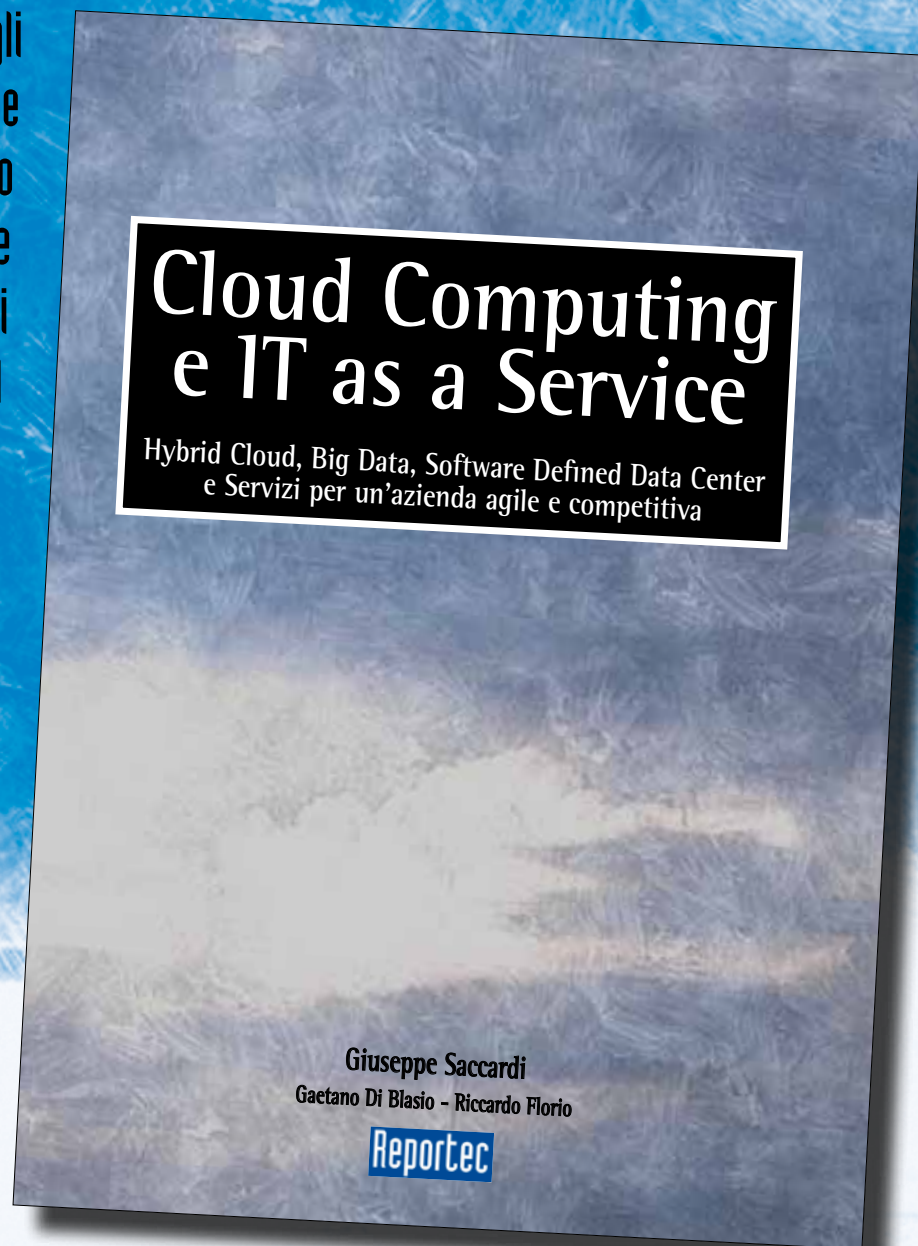
gli altri.

Questo spazio non è vincolante, o limitante. Esisterà un “logout”, oltre il quale tornare ad esercitare il nostro diritto di (presunta) anonimata. La sfida più difficile sarà quindi rendere consapevoli le persone di come bilanciare la propria esperienza in rete fuori e dentro lo spazio di cittadinanza, e rendere quest’ultimo realmente più interessante da utilizzare.



È disponibile il libro sul **CLOUD COMPUTING**

In oltre 280 pagine analizza gli economics e le strategie alla base dell'adozione del Cloud come strumento per rendere l'IT più efficace, razionale e meno costoso, nonché gli aspetti connessi ai nuovi paradigmi dell'IT e del cloud. Tra questi l'Hybrid Cloud, i Big data e il Software Defined Data Center. Completa l'opera l'esame della strategia e della proposizione di primarie aziende dell'IT internazionale che hanno fatto del Cloud uno degli elementi portanti del proprio portfolio di soluzioni e servizi.



Il libro è acquistabile al prezzo di 50 euro (iva e spese di spedizione incluse) richiedendolo direttamente a Reportec tramite:

mail to: info@reportec.it

oppure telefonando allo **02-36580441**

Check Point protegge i sistemi di controllo industriale

Le nuove soluzioni SCADA per proteggere i sistemi di controllo industriale contro le minacce della criminalità informatica



Ci sono alcune tipologie di attacchi che possono provocare danni non soltanto a delle aziende o istituzioni ma ad intere comunità. Per esempio nel caso di attacco a sistemi di controllo industriali (ICS – Industrial Control Systems) si possono avere ripercussioni sui sistemi di distribuzione dell'elettricità e dell'acqua e delle reti di trasporto. Ciò significa che un attacco informatico su questi sistemi, sia virtuale sia fisico, ha la potenzialità di bloccare l'intera rete elettrica di una comunità e di danneggiare i sistemi e le linee di produzione.

Gartner ha dichiarato che le continue violazioni alla sicurezza informatica delle infrastrutture porteranno a danni ambientali di oltre 10 miliardi di dollari, perdite di vite, e al livello globale all'introduzione di nuove regole. Il fornitore di sicurezza Check Point Software Technologies ha di recente esteso la sua soluzione di sicurezza per i sistemi di controllo industriali (ICS – Industrial Control Systems) con una nuova appliance 1200R security gateway grazie alla quale le aziende possono avere maggiore visibilità e controllo delle proprie reti SCADA, e potranno prevenire e rilevare le minacce alle reti stesse.

Check Point 1200R è un nuovo gateway di sicurezza specificamente costruito e reso robusto per essere utilizzato in ambienti difficili e installazioni remote in

condizioni analoghe a quelle che si trovano negli impianti di generazione e nelle sottostazioni di distribuzione dell'energia elettrica. L'appliance 1200R completa l'attuale famiglia di prodotti Check Point di sicurezza per i gateway ed è in grado di fornire la completa visibilità e controllo del traffico SCADA per prevenire gli attacchi alle reti, alle apparecchiature e ai processi logici.

I rapporti sulle minacce pubblicati dal Next Generation SmartEvent di Check Point forniscono dati completi sul traffico SCADA per consentire investigazioni dettagliate in caso di incidente. Grazie a Check Point Compliance Blade la soluzione garantisce anche il rispetto delle regole previste.

Le caratteristiche dell'Appliance 1200R di Check Point comprendono:

- Gateway di sicurezza Check Point completa con porte 6x1GbE e throughput del firewall di 2Gb/s
- I più completi protocolli ICS/SCADA disponibili, compresi Modbus, MMS, DNP3, IEC60870-5-104, IEC 61850, ICCP, OPC, BACnet, Profinet, Siemens Step7 e molti altri
- Dimensioni compatte, senza ventilatori o parti in movimento, la gamma di temperature operative, da -40°C e 75°C, supera gli standard.
- Rispetta le più stringenti specifiche: IEC 61850-3, IEEE 1613 e IEC 60068-2.

Cambiare approccio per proteggersi dagli attacchi mirati

di Riccardo Florio

L'opinione di Gastone Nencini, country manager di Trend Micro Italia sulla tipologia emergente di attacchi costruiti su misura

Nell'attuale scenario della sicurezza informatica, gli attacchi mirati rappresentano una minaccia emergente e in costante diffusione. Si tratta di una tipologia di attacco tra le più difficili da contrastare poiché utilizza tecniche sofisticate e diversificate, combinate in una strategia basata su più fasi e applicate con tenacia e continuità fino al conseguimento dell'obiettivo. Ce ne parla Gastone Nencini, country manager Trend Micro Italia: «Gli attacchi mirati sono rivolti ad aziende di ogni tipo e sono utilizzati in tutti gli ambiti: nello spionaggio industriale o governativo, nelle azioni di sabotaggio, nelle frodi, nei furti di proprietà intellettuale, nella sottrazione di dati e così via».

Il punto di partenze di un attacco mirato è la raccolta di informazioni sulla singola organizzazione target e sui soggetti indirettamente collegati a essa; tra questi ultimi possono esserci aziende partner, collaboratori o clienti dell'organizzazione sotto attacco, spesso aggirati con l'uso di tecniche di social engineering al fine di ottenere informazioni che, separatamente, possono sembrare poco rilevanti ma che, se correlate tra loro, possono fornire chiavi per la compromissione della sicurezza.

Una volta identificato l'elemento debole della catena, spiega ancora Nencini, (il computer di un dipendente, un dispositivo mobile aziendale, un server ...), l'attaccante ne sfrutta le vulnerabilità riuscendo spesso a eludere gli strumenti di protezione generali predisposti dall'azienda e a installare un malware. Questo primo sistema compro-

messo rappresenta il grimaldello su cui costruire le azioni successive, cominciando dalla predisposizione di un centro di comando e controllo per stabilire una comunicazione costante con l'host compromesso. A questo punto l'attaccante rimane per lungo tempo ad agire inosservato spostandosi all'interno della rete alla ricerca di sistemi che ospitano informazioni sensibili o in grado di fornire un accesso di livello superiore alle altre risorse di rete, analizzando le vulnerabilità ed espandendo la propria presenza e controllo. L'ultima fase è quella dell'attacco vero e proprio verso il target prefissato, che può proseguire indisturbata anche per mesi, durante la quale vengono sottratte informazioni chiave attraverso una backdoor, svuotando l'azienda di tutti i suoi asset. «Questa tipologia di attacco definita "tailor made" necessita di un sistema di difesa che sia anch'esso costruito su misura, capace di tenere conto delle vulnerabilità associate a ognuna delle fasi di attacco e che sia in grado di intercettarlo, bloccarlo e renderlo inattivo all'interno della rete», afferma Nencini. Servono meccanismi di difesa basati su analisi e correlazione degli eventi, in grado di operare in modo efficace e sinergico. Trend Micro affronta questa sfida con prodotti quali la suite Deep Discovery e il suo modello di Custom Defense, in grado di adattarsi allo specifico ambiente IT di ogni azienda.



Gastone Nencini -
Trend Micro

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**



Giuseppe Saccardi - Gaetano Di Blasio - Riccardo Florio

Reportec



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