

SECURITY

& BUSINESS

n.12
DICEMBRE 2012

**IN QUESTO
NUMERO:**

CRESCE IL RISCHIO SUL WEB SECONDO IBM X-FORCE

Sempre più pericoloso navigare sul Web. È quanto sottolineano i responsabili della divisione IBM Security, commentando i risultati "dell'X-Force 2012 Mid-Year Trend and Risk Report", che mostra un netto aumento degli exploit legati ai browser, una crescita delle minacce alla sicurezza delle password per l'accesso ai social media e ulteriori rischi relativi ai programmi aziendali BYOD. «Permettere alle aziende di stare un passo avanti alle minacce», è questo l'obiettivo del

rapporto, come spiega Kris Lovejoy, General Manager di IBM Security Services, la quale continua: «Le aziende oggi si confrontano con un panorama delle minacce in costante evoluzione. Il nostro team di analisi tiene traccia e monitora in modo capillare le minacce emergenti, fornendo una valutazione del panorama della sicurezza, ideata per aiutare le aziende a comprendere meglio i rischi più recenti e a superare tali minacce».

pag.6-7

SECURITY SUMMIT 2013

Giunto alla 5a edizione, il Security Summit torna a Milano dal 12 al 14 marzo 2013. Farà quindi una nuova tappa a Bari il 18 aprile, e poi a Roma il 5 e 6 giugno e infine a Verona il 3 ottobre.

Progettato e costruito per rispondere alle esigenze dei professionisti di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia

dal mondo imprenditoriale che da quello universitario e della ricerca, Security Summit si rivolge ai professionisti della sicurezza ma anche a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'ICT Security. Il Security Summit è organizzato dall'Associazione Italiana per la Sicurezza Informatica (CLUSIT) e da Cardi Eventi, la divisione "Conference" di Cardi Editore, organizzatore di eventi nel mondo finanziario e dell'Ict.

pag.8-9

CYBER WAR pag.05
• Attenti al falso Google

COMPLIANCE pag.10
• Il Garante rinnova le autorizzazioni generali

COMPLIANCE pag.11
• Internet cookie: più trasparenza in primavera

NEWS pag.12
• Trend Micro libera le aziende dalle preoccupazioni
• RSA apre un anti-fraud command center con la Purdue University
• Joint Venture tra Yarix e Biogy

SOLUZIONI pag.13
• Intel con Vasco per un accesso sicuro

SOLUZIONI pag.15
• BYOD: Fortinet risponde con FortiOS 5.0 e nuovi Asic

**LA PAROLA AI
PROTAGONISTI:
pag.16-17**

• Ibm Security punta "sull'intelligenza"

NEWS pag.18
• Nuovi servizi ThreathCloud di Check Point
• Il portale Dell SonicWall per conoscere minacce e sicurezza

È disponibile il libro sulla **SICUREZZA AZIENDALE**

È disponibile il libro "Sicurezza aziendale e continuità del business" realizzato da Reportec. In circa 300 pagine analizza le problematiche di governance e di risk management connesse con i diversi aspetti della sicurezza aziendale: dalla protezione delle informazioni, alla continuità operativa, alla salvaguardia degli asset fisici, non dimenticando di sottolineare le problematiche portate dagli ultimi trend tecnologici, come il cloud computing e la mobility. Completa il volume l'analisi delle soluzioni sviluppate da un ampio numero di primarie aziende del settore.



È anche disponibile il libro
UN'IMPRESA SEMPRE PIÙ MOBILE

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



Security & Business evolve. Nato come raccolta di notizie sulla sicurezza, ha cominciato a ospitare sempre più approfondimenti, anche sulla spinta dei lettori che si stanno aggiungendo numerosi, provenienti da vari ambiti: professionisti della sicurezza, ma anche dell'IT in generale e un crescente numero di business manager, consapevoli che la sicurezza è un "problema" per tutta l'azienda. Dal 2013, insisteremo sempre più in questa direzione e, anche per questo abbiamo aggiunto una nuova rubrica, frutto di un rapporto privilegiato che abbiamo sviluppato con il Security Summit, la manifestazione organizzata dal Clusit (la nota Associazione Italiana per la Sicurezza Informatica, nata in seno al dipartimento di Informatica dell'Università di Milano).

La nuova rubrica ospiterà contenuti relativi al Summit e al prezioso lavoro del Clusit che riteniamo di assoluto valore sul panorama tecnico-scientifico dell'ICT Security, ma non solo, essendo anche particolarmente attento a tutti gli aspetti normativi e alle ripercussioni sociali di questo tema centrale per le imprese e gli individui. Un lavoro che si sposa felicemente con le finalità di Security & Business: diffondere quanto più è possibile la cultura della sicurezza e la sua conoscenza.

Sin dalla fondazione, Reportec segue con continuità e attenzione il mondo della sicurezza e quello della continuità operativa. Negli anni abbiamo assistito alla costante crescita delle minacce e dei rischi, cercando di informare i nostri lettori attraverso i nostri report, le riviste e i libri. Security & Business è nato per fornire un aggiornamento continuativo, senza l'assillo delle newsletter quotidiane e, come detto, si vuole sempre più dedicare ad approfondire tali notizie. Oltre alla rubrica sul Security Summit, saranno protagoniste della rivista CyberWar, che da qualche numero fa un punto sulle ultime minacce, riportando le principali ricerche del settore e gli aspetti più impattanti sul lavoro. Compliance è la finestra sui provvedimenti legali e sarà sempre più attenta a situazioni reali. La parola ai Protagonisti fornirà opinioni e visioni da parte di personaggi chiave del settore.

Seguono poi approfondimenti a vario livello, presto anche multimediali, per sfruttare il formato elettronico scelto per la testata, su casi di studio, sulle tecnologie, sulle soluzioni. Per finire anche strategie e notizie sulle società che "vendono" sicurezza saranno presentate perché in un ambito così critico e delicato è fondamentale per un'azienda "conoscere" i propri fornitori.

SMAU

INNOVAZIONE DI CASA NELLE CITTÀ ★



SMART CITY ROADSHOW

È L'INIZIATIVA DI SMAU E ANCI DECLINATA IN CINQUE TAPPE SUL TERRITORIO ITALIANO PER VALORIZZARE E METTERE A FATTOR COMUNE LE INIZIATIVE EMERGENTI NEL NOSTRO PAESE, OGGETTO DEL TAVOLO DI LAVORO SMART CITY DELLA CABINA DI REGIA DEL GOVERNO, CHE DIVENTANO COSÌ PATRIMONIO A DISPOSIZIONE DELLA BUSINESS COMMUNITY PER COSTRUIRE LA "VIA ITALIANA ALLE CITTÀ INTELLIGENTI".

A SMAU, UN CICLO DI LABORATORI IN CUI PRESENTARE CASI DI SUCCESSO IN AMBITO SMART CITY, UN PREMIO DEDICATO, UN'AREA START UP E UN EVENTO ISTITUZIONALE PER DELINEARE LO SCENARIO DI MERCATO NAZIONALE E INTERNAZIONALE.

BARI
6-7 FEBBRAIO 2013

ROMA
20-21 MARZO 2013

PADOVA
17-18 APRILE 2013

TORINO
8-9 MAGGIO 2013

BOLOGNA
5-6 GIUGNO 2013

MILANO
16-18 OTTOBRE 2013



Smart City Roadshow porta direttamente "a casa" delle Pubbliche Amministrazioni del territorio progettualità innovative per trasformare le città in chiave Smart City. L'EVENTO È RISERVATO AGLI OPERATORI PROFESSIONALI - IMPRESE, AMMINISTRATORI PUBBLICI, MEDIA -

UN'INIZIATIVA DI

smau



www.smau.it



contact@smau.it



+39.02.283131



CONTATTI

ATTENTI AL FALSO GOOGLE

Il Web continua ad essere un luogo pericoloso e la tendenza non si fermerà nel 2013. L'emissione di un falso certificato di sicurezza di un'authority turca ha dato il via alla creazione di falsi siti del più noto motore di ricerca

L'errore è sempre in agguato. A causa di uno di questi, una certification authority turca ha emesso un certificato di sicurezza che ha permesso la creazione di certificati fasulli con i quali era possibile imitare vari siti di Google. In particolare, il 24 dicembre Chrome, il browser di Google, ha identificato e bloccato un certificato non autorizzato che avrebbe "garantito" la sicurezza di domini "*.google.com". Le indagini di Google hanno permesso di risalire all'errore di TurkTrust, che, dopo verifiche interne, ha annunciato di avere due certificati sbagliati nell'agosto del 2011.

Il problema è stato risolto e tutti i produttori di browser sono stati avvisati affinché i propri sistemi di navigazione venissero aggiornati per non riconoscere come validi tali certificati e quelli federati da questi. Peraltro gli aggiornamenti continueranno anche nelle prossime settimane e mesi, prima di potersi "fidare" completamente, vista la persistenza degli e-documents su Internet e la scarsa propensione agli aggiornamenti. La stessa Google ha annunciato ulteriori upgrade per Chrome in gennaio, come pure Mozilla per Firefox, ma è importante che i sistemi vengano lasciati liberi di aggiornarsi. Microsoft, peraltro, ha annunciato che i propri sistemi Vista, Windows 8 e Windows Server 2012 sono automaticamente protetti perché dallo scorso giugno dispongono della Certificate Trust List.

Quali danni si siano verificati è difficile saperlo, certo il rischio è stato grande, considerando la crescita degli attacchi tramite Web. I certificati falsi, infatti, possono essere utilizzati per effettuare attacchi di phishing o quelli cosiddetti "man-in-the-middle" (quelli in cui l'attaccante si posiziona senza essere visto tra due estremi di una "connessione",

intercettando ed eventualmente alterando i contenuti della stessa) o, ancora, per lo spoofing di contenuti (cioè la loro "falsificazione, per cui si ha la percezione di essere su un sito sicuro e accedere a determinati contenuti, mentre si è stati indirizzati su un sito falso che, insieme a contenuti magari reali perché copiati, vengono inconsapevolmente scaricati codici maligni).

Un 2013 rischioso

Il Web continuerà a essere "pericoloso" anche nel 2013, stando alle rivelazioni di alcuni specialisti della sicurezza (si veda anche il prossimo articolo), ma ancora più a rischio saranno gli ambienti mobili. Secondo i responsabili di McAfee, per esempio, proprio gli attacchi sui dispositivi mobili saranno la principale minaccia dell'anno prossimo. Qui, probabilmente, per gli hacker sarà meno difficile usare il Web, perché spesso il malware viene annidato in app che sembrano innocue e che vengono scaricate ingenuamente anche se riportano "diligentemente" tutto quello di cui sono capaci. In molti hanno scaricato (il ranking d'apprezzamento è alto) uno screen saver per dispositivi mobili che tra le sue funzioni dichiara (ma quanta fatica leggere le note!) di poter raccogliere e inviare dati dal device, compresi numeri di carte di credito ed effettuare telefonate verso numeri a pagamento. Al secondo posto tra le minacce ci sono i ramsoware (si veda lo scorso numero di Security & Business). Il denominatore comune è il profitto: quanto più è facile guadagnarci tanto più i malware vengono sfruttati, anche perché è sempre più facile reperirli nel cyber underground o, visto che va di moda il cloud, nel mondo HaaS (Hacking as a Service).

CRESCE IL RISCHIO SUL WEB SECONDO IBM X-FORCE

Il report su trend e rischi di metà anno evidenzia minacce emergenti che riguardano browser e social media, oltre a rischi persistenti nei dispositivi mobili e nei programmi BYOD



Fabio Panada di Ibm

Sempre più pericoloso navigare sul Web. È quanto sottolineano i responsabili della divisione IBM Security, commentando i risultati "dell'X-Force 2012 Mid-Year Trend and Risk Report", che mostra un netto aumento degli exploit legati ai browser, una crescita delle minacce alla sicurezza delle password per l'accesso ai social media e ulteriori rischi relativi ai programmi aziendali BYOD ("Bring Your Own Device").

«Permettere alle aziende di stare un passo avanti alle minacce», è questo l'obiettivo del rapporto, come spiega Kris Lovejoy, General Manager di IBM Security Services, la quale continua: «Le aziende oggi si confrontano con un panorama delle minacce in costante evoluzione, con tecnologie emergenti che rendono sempre più difficile gestire e proteggere i dati riservati. Il nostro team di analisi tiene traccia e monitora in modo capillare le minacce emergenti, fornendo una valutazione del panorama della sicurezza, ideata per aiutare le aziende a comprendere meglio i rischi più recenti e a superare tali minacce». Il rapporto raccoglie i dati da numerose fonti di informazioni, tra cui il database IBM di oltre 68mila vulnerabilità, il Web crawler globale di IBM e gli spam collector internazionali, nonché dal monitoraggio in tempo reale di 15 miliardi di eventi quotidiani, fornito come Managed Security Service a circa 4mila clienti in oltre 130 paesi attraverso i 10 Security Operations Centers globali di IBM.

Occhio al Web

Una prima tendenza confermata si riguarda l'aumento di malware e attività Web maligne. Gli hacker persistono nel

prendere di mira gli individui indirizzandoli verso un URL o un sito fidato, in cui è stato "nascosto" un codice maligno. Quest'ultimo viene installato sul sistema bersaglio sfruttando, in particolare, le vulnerabilità del browser. Purtroppo molti siti di organizzazioni affermate, considerate "trusted", sono ancora soggette a tali tipi di minacce.

Dal rapporto emerge anche la costante crescita nell'utilizzo dell'SQL injection, una tecnica utilizzata per accedere a un database tramite un sito Web. Allo stesso passo è l'incremento registrato dall'utilizzo di comandi cross-site scripting e directory traversal.

Social e Mobile sotto attacco

Sono i grandi numeri ad attrarre gli attacker, perché statisticamente nella massa è più facile colpire più bersagli. Per questo si moltiplicano gli attacchi legati ai social media e quelli che prendono di mira i dispositivi mobili. Aumentano gli attacchi, ma nel 2012 lo sviluppo di nuovi malware per smartphone è risultato in forte calo rispetto alla crescita esponenziale del passato. «Forse perché bastano quelli vecchi - ci spiega Fabio Panada, IBM Security Tech Sales Leader -. Grazie alla crescita delle politiche BYOD, questi dispositivi sono sempre più diffusi e usati in azienda, ma non sono "nati" per essere enterprise. I produttori non hanno processi di patching della sicurezza e neanche l'utente si pone il problema di doverla aggiornare. Al più migliorie in tal senso sono inserite nelle nuove versioni del sistema operativo, ma non vengono evidenziate e non ci sono sforzi dei produttori per far installare la nuova release».

L'ingenuità degli utenti è ancora la chiave più comoda: il report sottolinea, infatti, che per gli smartphone il rischio più grosso nella prima metà del 2012 è stato rappresentato dagli scam che inviano automaticamente SMS a numeri di telefono a tariffa maggiorata. Tali scam operano da applicazioni che vengono scaricate dall'utente da un app store, dove appaiono come clone di un'app reale oppure sembrano legittime ma non lo sono e, spesso, riportano anche tra le funzioni le attività maligne, che nessuno legge. Panada sottolinea anche che nessun sistema operativo è immune: «Ormai la diffusione dei dispositivi Apple rende "conveniente" sviluppare malware anche per questi ambienti, in particolare si nota la crescita di Advanced Persistent Threat (APT) ed exploit, che possono oggi competere con quelle di solito osservate sulle piattaforme Windows».

In aumento attacchi sofisticati e mirati, oltre che per i Mac, anche verso le password dei siti Web di social networking. Questo perché si è diffusa la connessione tra tali siti e servizi Web vari, come la mail o altri basati su cloud, attraverso un'esperienza integrata da dispositivo a dispositivo. In pratica, la stessa password viene condivisa, ma è necessario controllare come questi account sono collegati e preoccuparsi della sicurezza della loro password e dei dati privati che sono stati forniti per il recupero della password o il reset dell'account. La raccomandazione di X-Force è usare una password lunga, composta da più parole anziché da una scomoda combinazione di caratteri, numeri e simboli. Inoltre, dal lato server, X-Force esorta a crittografare le password di accesso ai database, utilizzando una funzione "hash" idonea alla memorizzazione delle password. La funzione "hash" deve essere difficile da decodificare e deve utilizzare un "salt value" per ogni account utente.

Nuovo Security Operations Center in Polonia

Fonte preziosa di informazioni per le ricerche di X-Force sono i Security Operations Center globali di Ibm. Recentemente, ne è stato inaugurato uno a Breslavia in Polonia. Si tratta del decimo, che, a detta dei responsabili di Ibm va a occupare una posizione strategica al centro dell'Europa. «IBM sta investendo attivamente nei mercati in crescita in tutto il mondo - spiega Anna Sienko, Country General Manager IBM Poland & Baltics - IBM ospita alcune delle più avanzate competenze informatiche del mondo: lo staff del nostro nuovo Security Operations Center di Breslavia entrerà a far parte di un team globale di esperti della sicurezza, che vanta competenza ed esperienza ineguagliate nell'aiutare le organizzazioni a comprendere e a rispondere meglio alle minacce per la loro attività».

IBM gestisce altri nove Security Operations Center globali: ad Atlanta in Georgia; Detroit in Michigan; Boulder in Colorado; Toronto in Canada; Bruxelles in Belgio; Tokyo in Giappone; Brisbane in Australia; Hortolandia in Brasile; Bangalore in India. Tutti i centri sono progettati per assicurare che i sistemi mission-critical, gli impianti elettrici, l'elaborazione dei dati e i collegamenti di comunicazione siano protetti da ogni single point of failure.

Qualche aspetto positivo

Il rapporto di Ibm X-Force, comunque, evidenzia anche alcuni progressi nella sicurezza di Internet. Per esempio, vi è un calo costante degli exploit rilasciati, miglioramenti da parte dei primi dieci fornitori sulle correzioni delle vulnerabilità e una riduzione significativa delle vulnerabilità relative al PDF (Portable Document Format). IBM ritiene che quest'area di miglioramento è direttamente correlata alla nuova tecnologia di sandboxing fornita dalla release Adobe Reader X.

Il sandboxing, in generale, si sta rivelando un investimento di successo dal punto di vista della protezione. Si tratta di una tecnica usata dagli analisti della sicurezza per isolare un'applicazione dal resto del sistema in modo tale che, quando questa dovesse venir compromessa, il codice dell'attacker eseguito all'interno dell'applicazione stessa non possa propagarsi all'esterno.

Gaetano Di Blasio

SECURITY SUMMIT 2013

Giunto alla 5a edizione, il Security Summit torna a Milano dal 12 al 14 marzo 2013. Farà quindi una nuova tappa a Bari il 18 aprile, e poi a Roma il 5 e 6 giugno e infine a Verona il 3 ottobre.

Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto.

Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, Security Summit si rivolge ai professionisti della sicurezza ma anche a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'ICT Security.

Il Security Summit è organizzato dall'Associazione Italiana per la Sicurezza Informatica (CLUSIT) e da Cardi Eventi, la divisione "Conference" di Cardi Editore, organizzatore di eventi nel mondo finanziario e dell'Ict.

Il programma convegnistico del Summit di Milano 2013

Al Summit di Milano, ogni giornata avrà una tematica principale di riferimento. La prima giornata sarà dedicata a Cybercrime/Intelligence/Cyber Warfare. In apertura, come keynote Speaker è previsto l'intervento di Steve Purser, Head of Technical Department di ENISA.

Durante il primo giorno si parlerà anche di: Sicurezza delle applicazioni Web, Evoluzione del malware, Monitoraggio, Spionaggio, Sabotaggio, Mobile security, SCADA Security, Nuovi strumenti di Autenticazione, Come realizzare e gestire un Security Operations Center, Mobile Forensic, Gestione delle Frodi in Azienda.

La seconda giornata sarà dedicata all'Agenda Digitale

Europea e italiana. In apertura, interverrà Alessandra Falcinelli, dell'European Commission - DG for Communications Networks, Content and Technology (CONNECT) Unit H.4 – Trust and Security.

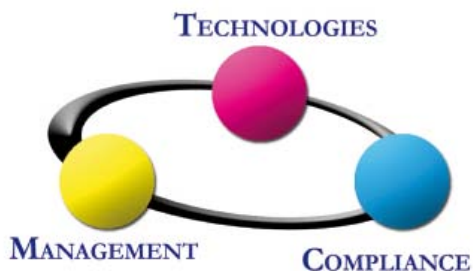
Durante il secondo giorno si parlerà anche di: Fascicolo Sanitario elettronico e Cartella Clinica elettronica, Sicurezza nei servizi delle Pubbliche Amministrazioni locali, metodologia MEHARI per l'analisi dei rischi, Security Convergence, Continuità operativa, Controllo degli accessi e gestione delle identità, La sicurezza e la gestione dei documenti, E-commerce, Sicurezza nelle transazioni finanziarie.

La terza giornata sarà dedicata al Cloud. In apertura, come keynote Speaker interverrà Jim Reavis, Executive Director, Cloud Security Alliance.

Durante la terza giornata si parlerà anche di: Disposizioni in tema di obbligo di comunicazione sulle violazioni di dati personali, Contraffazione, pirateria, violazione dei diritti d'autore, Disaster Recovery, Storage, La sicurezza nei Data Center, Social Media Security, Standard di sicurezza; il mestiere del CISO, Certificazioni Professionali, Computer Forensics.

Attestati, Crediti CPE e Diplomi

Tutte le sessioni prevedono il rilascio di Attestati di Presenza e l'attribuzione di crediti/ore CPE (Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP, CISA, CISM o analoghe richiedenti la formazione continua. A chi avrà assistito a tre sessioni appartenenti a uno stesso Percorso Professionale (tecnico,



legale o sulla gestione della sicurezza), sarà rilasciato un Diploma.

Il Rapporto Clusit

Nel 2012 il Clusit ha dato vita al primo "Rapporto sulla sicurezza Ict in Italia", un volume di 148 pagine che, attraverso il lavoro di oltre un centinaio di professionisti e il coinvolgimento di più di 150 aziende, ha tracciato un profilo neutrale e approfondito della situazione sulla sicurezza Ict nel nostro Paese. È in corso di realizzazione il Rapporto 2013, che sarà presentato il 12 marzo a Milano. Insieme alla consueta analisi dei fatti più significativi (cybercrime e incidenti informatici) del 2012 in Italia e nel mondo, il Rapporto conterrà le tendenze del mercato e degli investimenti in Italia e le tendenze del mercato del lavoro. Tra i Focus On, si affronteranno alcuni temi di grande attualità: L'Agenda Digitale Italiana; lo stato della sicurezza ICT nella sanità in Italia; sicurezza e affidabilità, fattori indispensabili per lo sviluppo del commercio elettronico. Ma si parlerà anche di: Mobile, Social media, Cloud, Ipv6, Conservazione dei dati-backup, Security Operations Center (SOC), come è diversamente percepita la security in Italia e nel mondo.

Hacking Film Festival – Milano, 12 e 13 marzo

Al termine delle due prime giornate, nelle sale del Summit si terrà la quinta edizione dell'Hacking Film Festival. Saranno proiettate opere che illustrano "dall'interno" l'ambiente e il fenomeno hacker, i casi giudiziari più importanti che hanno attraversato il panorama tecnologico underground e le problematiche di sicurezza e vulnerabilità dei sistemi. Le proiezioni saranno seguite da un ampio dibattito, coordinato



da alcuni dei maggiori esperti presenti al Security Summit. Al termine, gli spettatori sono invitati a partecipare a un aperitivo.

Per altre informazioni:

Agenda e contenuti Security Summit 2013:
info@clusit.it, +39 349 776 8882.

Altre informazioni:

ceventi@cardieditore.com, +39 335 6528130.

Video riprese e interviste precedenti edizioni:
<http://www.youtube.com/user/SecuritySummit>

Foto reportage:

<http://www.facebook.com/group.php?gid=64807913680&v=photos>

Sito web: <http://www.securitysummit.it/>
 Security Summit Milano 2012:

<http://milano2012.securitysummit.it/>

Security Summit Roma 2012:

<http://roma2012.securitysummit.it/>

Security Summit Verona 2012:

<http://verona2012.securitysummit.it/>

La partecipazione al Security Summit ed a tutte le attività è libera e gratuita, con il solo obbligo dell'iscrizione online.



IL GARANTE RINNOVA LE AUTORIZZAZIONI GENERALI

Primarie e mediazione civile le novità, mentre per gli altri dati sostanzialmente riconfermate le precedenti disposizioni

Dal 1° gennaio sino al 31 dicembre 2013 saranno efficaci le nuove autorizzazioni al trattamento dei dati sensibili secondo quanto stabilito dal Garante il 28 di dicembre 2012 e in via di pubblicazione sulla Gazzetta Ufficiale.

I provvedimenti riguardano i rapporti di lavoro, i dati sulla salute e la vita sessuale, le associazioni e le fondazioni, i liberi professionisti, le attività creditizie, assicurative, il settore turistico, l'elaborazione dei dati effettuata per conto terzi, gli investigatori privati e il trattamento dei dati di carattere giudiziario. In massima parte, le modifiche apportate, secondo quanto riportato dall'authority, non sono significative, perché si limitano alle necessarie integrazioni derivanti da modifiche normative intervenute nei settori considerati.

Ci sono però novità: la prima è relativa alle primarie che si sono svolte o si svolgeranno e per le quali il Garante ha ritenuto opportuno esplicitare in via generale le indicazioni finora fornite in occasione di singole competizioni, autorizzando, nell'ambito di quella riguardante gli organismi associativi e i partiti, anche il trattamento dei dati personali effettuato in occasione delle operazioni connesse allo svolgimento delle elezioni primarie.

La seconda novità riguarda la mediazione civile: nell'ambito delle autorizzazioni generali n. 5 (sul trattamento dei dati sensibili da parte di diverse categorie di titolari) e n. 7 (sul trattamento dei dati a



carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici) sono stati infatti contemplati anche i trattamenti di dati legati all'attività svolta dagli organismi di mediazione, già oggetto di due separate autorizzazioni ad hoc rilasciate dal Garante al momento dell'entrata in vigore della nuova disciplina sulla conciliazione delle controversie civili e commerciali. Si è realizzata in tal modo una semplificazione per gli operatori del settore che dispongono ora di un quadro più organico di riferimento.

Il Garante ha rinnovato, inoltre, l'autorizzazione generale al trattamento dei dati genetici e quella relativa al trattamento dei dati personali effettuato per scopi di ricerca scientifica, anch'esse efficaci sino al 31 dicembre 2013.

Le nuove autorizzazioni sono in corso di pubblicazione sulla Gazzetta Ufficiale.



INTERNET COOKIE: PIU' TRASPARENZA IN PRIMAVERA



Il Garante sul trattamento dei dati ha avviato una consultazione per raccogliere contributi di gestori e consumatori entro 90 giorni

Le “naviganti” avranno la possibilità di decidere se e come far usare i dati rilevati dai siti Web visitati per ricevere pubblicità mirata. Il Garante per la protezione dei dati personali ha infatti avviato le attività previste dalla direttiva europea 2009/136, recepita di recente in Italia, e ha avviato una consultazione pubblica (Pubblicato sulla Gazzetta Ufficiale n. 295 del 19 dicembre 2012) diretta a tutti i gestori, grandi e piccoli, dei siti e alle associazioni maggiormente rappresentative dei consumatori allo scopo di acquisire contributi e suggerimenti per arrivare a promulgare direttive in merito.

Per chi non lo sapesse, i cookie sono file di testo con informazioni su quanto visualizzato che vengono scaricati sul terminale usato per navigare.

Successivamente vengono utilizzati durante la visita o a quelle seguenti per eseguire azioni “coerenti” con gli interessi manifestati nelle visite al sito stesso e “ottimizzare”, così, l’esperienza di ciascun utente.

In altre parole, i cookie contengono informazioni molto utili alle aziende per attività commerciali, ma possono contenere anche informazioni sensibili. I principali browser consentono già di bloccare i cookie.

L’obiettivo dichiarato dal Garante è quello di definire un’informativa semplice, chiara e di immediata comprensione sull’uso dei cookie per aiutare gli utenti di Internet a decidere liberamente e consapevolmente.

Prime indicazioni sulle principali questioni in materia di cookie, intanto, sono disponibili nell’area Faq sul sito del Garante (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2142939>). Le proposte relative all’informativa semplificata potranno essere inviate all’Autorità per posta o in via telematica alla e-mail consultazione-cookie@gpdp.it.

Il Garante si è riservato di valutare anche eventuali proposte che potrebbero pervenire da università e centri di ricerca.

Cookie liberi e no

È bene sottolineare, che le nuove regole europee permettono di utilizzare i cookie “tecnici” anche senza un consenso specifico, ma i gestori dei siti hanno l’obbligo di informare gli utenti della loro presenza in maniera il più possibile semplice, chiara e comprensibile. Il che non è così scontato.

Per i cookie “non tecnici”, cioè quelli che raccolgono dati personali e consentono così la costruzione di un dettagliato profilo del consumatore, invero la maggior parte, le nuove regole prevedono l’obbligatorietà del consenso preventivo e informato dell’utente. In altre parole, i gestori dei siti non possono, dunque, installare cookie per finalità di profilazione e marketing sui terminali degli utenti senza averli prima adeguatamente informati e aver acquisito un valido consenso.

TREND MICRO LIBERA LE AZIENDE DALLE PROCCUPAZIONI

Il servizio Worry-Free Business Security Services di Trend Micro protegge ora anche pc Mac e dispositivi mobili, oltre a essere pronto per Windows 8 e Windows Server 2012. Si tratta della versione 5 di un servizio che rinnova l'impegno di Trend Micro verso le piccole e medie imprese, lanciato otto anni fa.

Parte dei servizi gestiti per la sicurezza, Trend Micro Worry-Free Business Security Services assicura protezione alle piccole e medie imprese, qualunque sia l'ambiente in cui sono connesse (Windows, Mac e Android), attraverso una console sicura basata sul Web. Le aziende, come evidenziano in Trend Micro, possono gestire tutti i loro dispositivi ovunque si trovino, nella certezza che le loro informazioni resteranno sempre al sicuro. Facendo leva sulla Trend Micro Smart Protection Network ed erogato sotto forma di servizio di sicurezza basato sul cloud, il Worry-Free (letteralmente libero da preoccupazioni) garantisce ai dispositivi un accesso costante

alle più recenti informazioni sulle minacce in circolazione, proteggendo ogni secondo milioni di grandi aziende, piccole imprese e utenti privati in tutto il mondo, come sottolineano i responsabili della società.

Nella versione 5, Worry-Free Business Security Services v5 presenta: supporto per Mac e dispositivi mobili; supporto per Windows 8 e integrazione con Windows Server 2012 Essentials; gestione flessibile dei dispositivi; workflow potenziati per ridurre i passaggi necessari a completare le attività comuni; un'interfaccia rivista per migliorare la facilità d'uso. Trend Micro Worry-Free Business Security Services ha una console di gestione basata sul Web e non richiede l'installazione su un server. Il costo per utente varia in base al numero di postazioni e il prezzo diminuisce al crescere dei volumi. Il servizio è disponibile anche con una formula di abbonamento mensile nell'ambito del programma per Managed Service Provider di Trend Micro.

RSA apre un anti-fraud command center con la Purdue University

Con un nuovo Anti Fraud Command Center (AFCC), la RSA, security division di EMC, espande le proprie attività globali per contrastare il cyber crime. Grazie alla collaborazione con la Purdue University, il nuovo centro è composto da un team di analisti, esperti di frodi, che lavorano per rilevare, tracciare, bloccare e sconfiggere gli attacchi di phishing, pharming e su app mobili perpetrati dai criminali online. L'RSA AFCC della Purdue University si fonda su partnership già avviate con oltre 13.000 provider di servizi di web hosting, noti sviluppatori browser e ISP per contrastare e garantire la chiusura di siti di phishing il più rapidamente possibile.

Situato vicino al campus principale del Purdue Research Park a West Lafayette, il nuovo AFCC di RSA rafforza il servizio RSA FraudAction che, secondo quanto riportato dalla società, ha finora arginato oltre 750mila attacchi online a livello globale. Al centro lavoreranno studenti altamente qualificati del dipartimento di Informatica della Purdue University che saranno formati, supervisionati e supportati dallo staff RSA.

Joint venture tra Yarix e Biogy

Yarix Sicurezza Informatica, società italiana attiva a livello europeo nell'ambito dell'information security, e Biogy, azienda americana specializzata in biometria e cybersecurity, uniscono le proprie competenze creando la joint venture Yarix Biogy con sede a Londra, dedicata alla ricerca e produzione di security token innovativi. Indirizzati a dati e transazioni bancarie i nuovi dispositivi dovranno garantire che gli acquisti online e le operazioni bancarie di aziende e privati vengano effettuati in completa sicurezza. «Negli ultimi anni è stato registrato in Italia un sensibile incremento dell'e-commerce – dichiara Mirko Gatto, CEO di Yarix – Ma persiste una diffusa diffidenza del consumatore italiano nei confronti dei pagamenti online, ritenendoli poco sicuri». Gatto ritiene ci siano dunque grandi opportunità, ma, per il momento preferisce non divulgare ulteriori dettagli relativi al progetto della neonata joint venture.



Alfredo Gatto
di Yarix



INTEL CON VASCO PER UN ACCESSO SICURO

Le tecnologie di Intel e Vasco consentono a Infocert di offrire un accesso sicuro a siti e servizi di posta elettronica certificata



Danilo Cattaneo di Infocert



Richard Zoni di Vasco

La soluzione di strong authentication MyDigiPass di Vasco, integrata nei processori Intel e appoggiata al cloud, è alla base di un servizio innovativo di Infocert per la firma "digitale" qualificata

Un nuovo servizio semplifica l'accesso a siti e servizi di posta elettronica certificata. Grazie alla collaborazione tra Intel e Vasco, infatti, è possibile sfruttare una strong authentication a due fattori: come quelle tipiche dell'home banking, che si basano su qualcosa che si possiede (la "chiavetta" digitale o, più correttamente, il token) e una che si conosce (la combinazione userID e/o password). Basato sulla tecnologia MyDigiPass di Vasco e su quella Identity Protection Technology (IPT) di Intel, il servizio consente a qualsiasi sito Web di fornire un accesso sicuro autenticato e permette agli utenti di unificare l'accesso a più servizi Web, a partire da Facebook o dalla propria posta elettronica, in modo da utilizzare un solo sistema garantito da una password "usa e getta" non riutilizzabile, ma senza la scomodità di un token.

Il servizio, infatti, ci spiega Richard Zoni, Sales Manager Italia di Vasco, coniuga l'integrazione di MyDigiPass sulla mother board Intel, sotto forma di firmware che si appoggia al servizio cloud MyDigiPass, con la tecnologia IPT. Quest'ultima, in particolare, prevede l'immissione della password in modalità sicura, impedendo a eventuali codici maligni (come i keylogger) di catturare la sequenza di tasti digitati.

La disponibilità della soluzione Vasco sui chip Intel rappresenta un ulteriore canale di vendita per lo specialista belga dell'autenticazione: «Omnipresent MyDigiPass diventa facile da integrare, non richiedendo necessariamente né un token né lo sviluppo di codice, conveniente e altamente sicuro, fornendo uno strumento unico di login a ogni applicazione», spiega Zoni annunciando l'obiettivo di distribuire entro il 2014 fino a 1 miliardo di DigiPass, tra quelli forniti dalle banche, vari provider e appunto quelli sui pc carrozzati da Intel con la nuova tecnologia. In particolare, Vasco MyDigiPass è disponibile su tutti gli Ultrabook e sui pc dotati di tecnologia Intel Vpro, come evidenzia Alberto Fabiani, Software & Corporate Resellers Regional Business Manager di Intel Italia & Svizzera.

A livello applicativo, in particolare, un'anteprima mondiale sarà a breve l'aggiornamento del servizio di posta certificata Legalmail annunciato dall'italiana Infocert, certification authority e provider di servizi per la sicurezza, quali firma digitale e PEC, per citare i più noti.

Legalmail sarà disponibile con un'autenticazione data dalla suddetta combinazione di MyDigiPass e di Intel IPT, che porterà vantaggi agli utenti in termini di maggiore sicurezza e una «migliore customer experience, grazie alla maggiore comodità d'uso», come sottolinea il direttore generale di Infocert, Danilo Cattaneo.

Gaetano Di Blasio

È disponibile il libro 2012 sul **CLOUD COMPUTING**

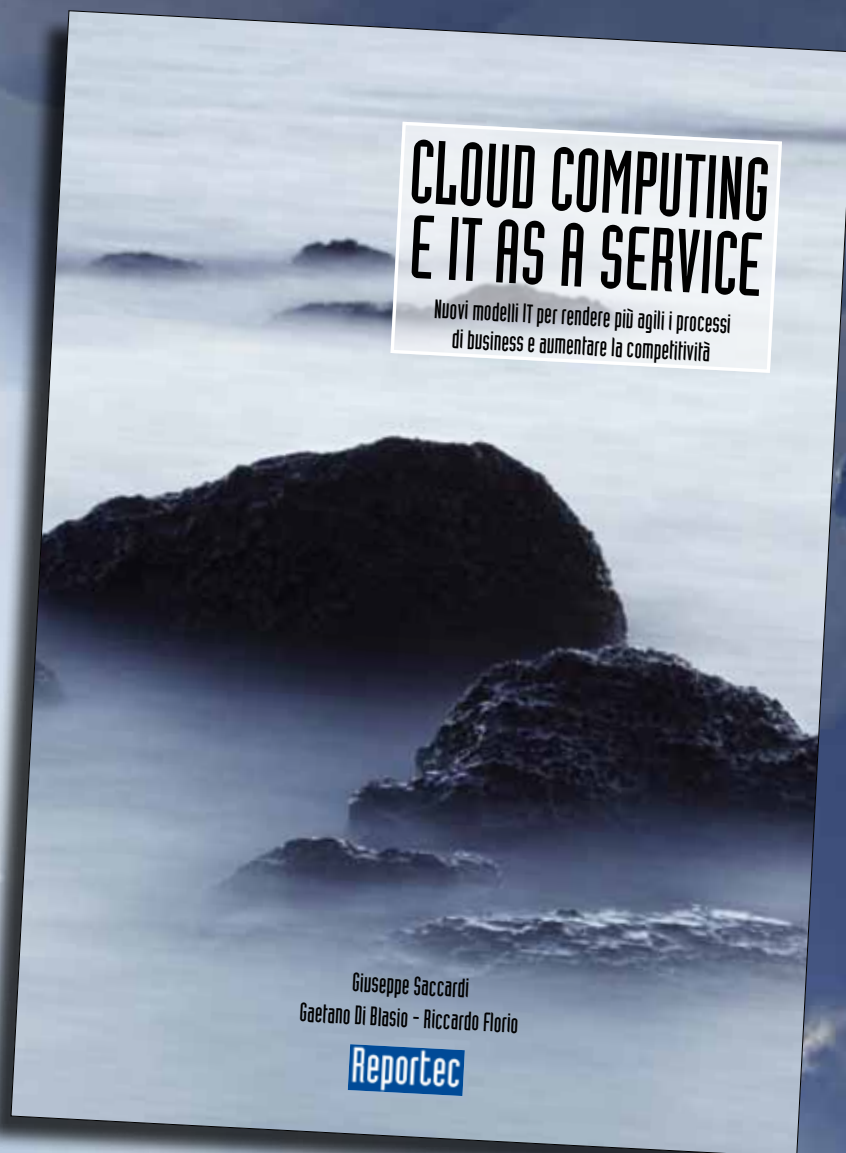
Realizzato da Reportec, in oltre 350 pagine analizza i prodromi del Cloud Computing, le modalità di fruizione e i benefici che derivano dall'adozione di questa innovativa possibilità di utilizzo del più avanzato IT senza dover immobilizzare ingenti capitali.

Completa il volume l'analisi delle soluzioni sviluppate per il Cloud Computing da parte di un ampio numero di primarie aziende del settore attive nel campo delle infrastrutture, delle applicazioni e dei servizi.

Il volume è uno strumento unico in Italia per affrontare le tematiche del Cloud Computing e approfondire gli aspetti, bilanciando i concetti e la teoria con quanto di concreto attualmente esistente.

Conoscere è infatti la condizione sine qua non perché un manager possa decidere. Questo obiettivo è perseguito mediante un esame analitico degli aspetti più importanti, gli

economics e le modalità di realizzazione e di adozione di un'infrastruttura Cloud Computing.



È anche disponibile il libro
UN'IMPRESA SEMPRE PIÙ MOBILE

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



BYOD: FORTINET RISPONDE CON FORTIOS 5.0 E NUOVI ASIC

Più sicurezza, controllo e “intelligenza” grazie alle 150 nuove caratteristiche del sistema operativo

Rispetto al solito, 150 nuove feature sono poche, esordisce Joe Sarno, Regional Sales Vice President di Fortinet, presentando la release 5.0 di FortiOs, ma spiega: «La 5.0 consolida i numerosi sviluppi realizzati negli ultimi anni a partire dalla 4.0 e le nuove caratteristiche sono “solo” le aggiunte necessarie». Aggiunte che vanno a indirizzare essenzialmente tre aree: «La protezione dalle minacce avanzate di nuova generazione, la sicurezza dei dispositivi mobili in risposta al fenomeno del BYOD (Bring Your Own Device) e una gestione “intelligente” delle security policy e della reportistica».

Sarno prosegue rivendicando per Fortinet la primogenitura di un firewall avanzato in grado di fornire protezione da più minacce e di mantenere contemporaneamente elevate le prestazioni di rete. Le caratteristiche di FortiOS 5.0 e la seconda generazione di FortiASIC-SoC2 si combinano per proseguire in questa tradizione, secondo quanto afferma il manager: «L’architettura dei nuovi ASIC fornirà eccezionali prestazioni di sicurezza di rete con accelerazione hardware per le appliance FortiGate. Ma i clienti che dispongono di modelli relativi agli ultimi due anni potranno aggiornare il sistema alla 5.0 gratuitamente e godere di tutti i vantaggi garantiti dal nuovo sistema».

Le nuove caratteristiche

Scendendo un po’ più in dettaglio, il nuovo software di sicurezza aggiunge alle appliance Fortinet capacità avanzate di identificazione e gestione del comportamento di utenti e dispositivi, inclusi criteri basati sulla reputation. In pratica, «identificato il dispositivo che chiede accesso alla rete, gli viene assegnato un punteggio, verificando il tipo di utilizzo, le applicazioni che contiene e altre caratteristiche – spiega

Sarno –. Un punteggio che rappresenta la reputazione del dispositivo, cioè il suo stato di sicurezza rispetto alle attività che l’utente vi opera». Più precisamente, per garantire una protezione adeguata all’evoluzione delle minacce, il nuovo sistema di rilevamento malware (in grado di ispezionare il traffico crittografato) comprende una engine euristica, basata sul comportamento, sul dispositivo e servizi antivirus basati su cloud, inclusi una sandbox del sistema operativo e un database della IP reputation dei botnet. «Il collegamento ai servizi cloud permette di anticipare le minacce, osservando in tempo reale gli eventi sulla Rete mondiale», sottolinea il manager, che aggiunge: «Il sistema applica quindi il profilo adeguato per dispositivo/utente, il tutto in maniera trasparente per l’utente stesso che non deve fare nulla». In pratica, il profilo viene definito in base al ruolo, ma anche al dispositivo utilizzato e ai dati e applicazioni cui si chiede accesso, con un adattamento automatico. L’affidabilità del sistema, come evidenzia ancora Sarno, consiste nella capacità di identificazione e autenticazione del dispositivo/utente, potenziata dall’utilizzo di uno strumento proprietario, denominato Captive Portal, che si aggiunge ai vari sistemi standard (Active Directory, Radius, 802.1X), alle funzioni del FortiClient e al supporto degli ambienti Citrix. È poi disponibile il profilo “guest”, che consiste in un accesso temporaneo alla rete: si evita, così, che un visitatore possa riutilizzare i parametri di accesso una seconda volta, magari entrando solo nell’atrio dell’edificio aziendale o che un consulente esterno possa accedere alla rete aziendale anche dopo aver terminato il lavoro (troppo spesso si dimentica di cancellare tali tipologie di utenti).

Tra le altre novità evidenziate da Sarno, l’enhanced IPv6, il wireless mesh che mancava, il local bridge mode per siti remoti, supporto SSID e port bridging. Importante anche l’update in tempo reale delle signature relative ai software di protezione di terze parti.

Oltre al nuovo sistema operativo FortiOS 5.0 per i dispositivi FortiGate, Fortinet ha annunciato FortiManager 5.0, FortiAnalyzer 5.0 e FortiClient 5.0 per aumentare la capacità di analisi e gestione dell’infrastruttura di rete e dei dispositivi endpoint di aziende e operatori di telefonia. L’aggiornamento alla versione 5.0 è automatico: una volta che sul FortiGate viene attivato il FortiOs 5.0, tale gateway provvederà ad aggiornare gli altri dispositivi non appena accedono alla rete.

Gaetano Di Blasio



IBM SECURITY PUNTA "SULL'INTELLIGENZA"

Nuove strategie e nuove soluzioni rinnovano l'approccio olistico basato su un framework che copre le esigenze aziendali a 360 gradi

Anche se c'è ancora chi non associa il marchio IBM agli specialisti della sicurezza, l'azienda americana ha investito molto in questo settore «crescendo sia tramite acquisizioni, sia attraverso ricerca e sviluppo», come sottolinea Tom Turner, vice president Marketing IBM Security Strategy e Security Intelligence.

A proposito di acquisizioni il manager ne ricorda due in particolare. La prima, che ha segnato l'inizio della strategia di crescita sulla sicurezza, è Internet Security Systems acquistata nel 2006. Turner ne vuole sottolineare i nuovi successi tecnologici cui ISS aveva abituato i propri utenti in passato: «ISS è tornata. Nell'ultimo test indipendente di InformationWeek il nuovo IPS XGS 500 (specificatamente pensato per la protezione da minacce provenienti da social network) è risultato primo». La seconda, finalizzata nel 2011, è l'ultima in ordine di tempo ed è proprio quella Q1Labs da cui Turner proviene e che rappresenta la punta di diamante della nuova strategia d'offerta di IBM sulla sicurezza.

L'intelligence e la strategia aziendale

È infatti di Q1Labs la tecnologia di "security intelligence", anch'essa premiata da InformationWeek, che costituisce uno dei principali elementi differenzianti di IBM: «Nel mercato della sicurezza, quando si incontrano i clienti, ci sono due tipi di conversazioni. La prima è con chi già dispone di un sistema per la security e cerca una specifica soluzione e, normalmente, avviene con un interlocutore "tecnico" – spiega Turner -. Il tema è il prodotto. Nella seconda, invece, il tema sono i nuovi trend, come il BYOD, la mobility, il

cloud, il social. Qui gli interlocutori sono sempre più spesso figure aziendali diverse dalle solite. Uomini di business che devono definire delle strategie, avviare dei progetti. La sicurezza è un elemento fondamentale di questi ultimi e il tema della security intelligence, che significa "controllo" e, in particolare, controllo del rischio, è un argomento vincente».

Interlocutori diversi rispetto a un recente passato che testimoniano un cambiamento di mentalità in atto nei confronti della sicurezza: «In un'azienda specializzata in trading finanziario nostra cliente, sono presenti tre figure legate alla sicurezza, ma nessuna riporta al Cio, bensì tutte rispondono direttamente al Ceo».

Due divisioni per un focus maggiore

Gli sforzi di IBM in termini di prodotto sono notevoli, considerato il portfolio molto ampio che copre ogni aspetto strategico sulla sicurezza. Ma la tecnologia è "solo" l'ultimo tassello di una strategia raffinata con il lancio di due nuove divisioni indipendenti, tra le quali sono state divise le attività riguardanti la sicurezza: IBM Security Systems e IBM Security Services.

«Stiamo investendo molto nella sicurezza. Aver definito due divisioni di brand, in cui operano oltre 6mila persone, lo dimostra», sottolinea Turner, che aggiunge: «Due divisioni che ci consentono di operare meglio sul mercato, perché testimoniano l'indipendenza dell'offerta prodotti rispetto ai nostri partner e perché consentono anche ai nostri esperti dei service di essere più indipendenti e non aver problemi a gestire servizi che



utilizzano soluzioni di altri specialisti della sicurezza». L'esperienza e la competenza dei propri specialisti, a cominciare dai ricercatori del team IBM X-Force, è uno dei punti di forza su cui fa leva IBM. Innanzitutto, il lavoro di X-Force, che è tra i gruppi di ricerca che scopre le vulnerabilità e i metodi per prevenirne lo sfruttamento prima di altri, viene trasferito nei prodotti per garantire una prevenzione "0-day" o precedente. In altre parole, prima ancora che vengano annunciate le vulnerabilità, i clienti di IBM sono già protetti dagli attacchi che le sfruttano. In secondo luogo, le suddette competenze vengono tradotte in best practice e applicate in tutto il mondo: «Le norme previste dal Garante italiano, coincidono in buona parte con quelle previste da altri regolamenti e leggi all'estero. Si tratta di problematiche che abbiamo già affrontato e che vengono risolte con l'apporto di ogni esperienza», evidenzia Turner, che continua: «Esperienza che è alla base dell'integrazione, caratteristica fondamentale della nostra offerta. È integrata "l'intelligenza", cioè vengono correlate tutte le informazioni raccolte in migliaia di reti e dispositivi nel mondo. È integrata la ricerca di X-Force. È integrata la protezione, che si basa sulla correlazione degli eventi in tempo reale per scovare e bloccare specifiche minacce e i vari tipi di attacchi exploit, valutando le anomalie e facendo convergere le azioni su tutti i gateway di sicurezza».

Dalla teoria alla pratica

Un'esperienza che si traduce in protezione e servizi all'avanguardia per i propri clienti, secondo Turner: «IBM dispone di un ampio portfolio di prodotti, soluzioni e servizi, che coprono tutte le esigenze descritte dal nostro security framework e divise per ambito in persone, dati, applicazioni, infrastrutture». Questo grazie alle soluzioni di Security intelligence e analytics a supporto di una stra-

tegia orientata a governance, rischio e compliance.

Una combinazione che permette a IBM, come spiega Turner, di coprire in particolare le macro tendenze del momento: la security intelligence, appunto, il cloud computing, le advanced threat, la mobility, la protezione delle identità e la compliance. Argomenti sensibili per lo staff IT, come per il business, per ciascuno dei quali Turner evidenzia alcuni casi reali, senza poterne, per ovvi motivi di riservatezza, citarne i nomi. Per esempio, una nota multinazionale del software, con 110mila dipendenti e oltre 15mila dispositivi da monitorare utilizza la Security Intelligence di QRadar, per ottenere piena visibilità sulla sicurezza in tempo reale. La piattaforma QRadar, più precisamente, consiste in un sistema SIEM (Security Information Event Manager) di ultima generazione e va a sostituire, nell'offerta IBM, il pur quotato Tivoli Siem. Quest'ultimo sarà supportato ancora a lungo, ma agli utilizzatori viene proposto comunque un programma di migrazione a QRadar, in grado di applicare analisi predittive ai dati e, soprattutto, capace di supportare la complessità crescente degli ambienti di oggi e la scalabilità necessaria per analizzare in streaming flussi di miliardi di dati. Soprattutto in grado di ridurre da 1 milione a 1 il numero di eventi cui prestare attenzione.

Una compagnia di telecomunicazioni internazionale, invece, gestisce privilegi di accesso per 250 specifici utenti nel mondo, per ciascuno rispettando la compliance locale. Per quanto riguarda le Advanced Threat, Turner sottolinea come non possano essere prevenute con un solo prodotto ed enfatizza l'apporto di IBM su tutti gli aspetti della sicurezza. Tra questi anche il cloud, che vede IBM impegnata sia per assicurare la sicurezza del cloud, sia come fornitore di servizi nel cloud. Anche per quanto riguarda la mobility, l'offerta di IBM è completa e sfrutta tecnologie all'avanguardia per la sicurezza degli endpoint.

NUOVI SERVIZI THREATCLOUD DI CHECK POINT

Per proteggersi dalle minacce sfruttando l'esperienza e la tecnologia di Check Point Software Technologies Sono ora disponibili nuovi specifici servizi, denominati Check Point ThreatCloud Security Services. Supporto continuo 24x7, protezione dalle minacce di ultima generazione, monitoraggio degli eventi direttamente sui gateway di sicurezza del cliente, il tutto con il supporto dell'infrastruttura di security intelligence ThreatCloud di Check Point, costituita da un network di collaborazione particolarmente esteso. Queste le caratteristiche dichiarate dai responsabili della società israeliana. I nuovi servizi includono ThreatCloud Managed Security Service e ThreatCloud Incident Response. Il primo monitora costantemente le reti e i gateway dei clienti alla ricerca di eventi di sicurezza e fornisce alert basati su dati specifici, che possono essere utilizzati per rispondere in modo efficace. Inoltre, aiuta a ottimizzare la sicurezza con una serie di indicazioni e suggerimenti sulle policy di Threat Prevention aziendali. ThreatCloud Incident Response, invece, fornisce ai clienti assistenza qualificata in tempo reale in

caso gli incidenti di sicurezza, aiutando le aziende a reagire prontamente.

Più in dettaglio, Check Point ThreatCloud Managed Security Service blocca gli attacchi abbinando tecnologia e analisi da parte di esperti. Inoltre, è in grado di calibrare le policy per le Software Blade di Threat Prevention firmate Check Point: IPS, Anti-Bot e Antivirus. Check Point ThreatCloud Incident Response fornisce il supporto di professionisti della sicurezza certificati da Check Point, quali sono sempre disponibili per raccomandare controlli e soluzioni pratiche di sicurezza, oltre che per implementare best practice specifiche. Il servizio, spiegano in Check Point, permette di accelerare i tempi di ripristino dopo un evento, consentendo alle aziende di tornare a operare a pieno regime in poco tempo. Mette inoltre a disposizione esperti on-call per proteggere la rete in caso di preparazione di un attacco o quando questo è già stato sferrato con successo e individuato. Il servizio permette anche di mitigare possibili eventi di sicurezza futuri con consigli post-incidente.

IL PORTALE DELL SONICWALL PER CONOSCERE MINACCE E SICUREZZA

La conoscenza è il primo fondamentale passo per la sicurezza. Per questo, Dell SonicWall ha messo a disposizione di tutti un portale che esamina in tempo reale le principali minacce nel Web e fornisce informazioni dettagliate sulle novità nel campo della sicurezza informatica.

Il portale include diverse sezioni, tra cui il Threat Center, che fornisce una panoramica in tempo reale delle minacce rilevate da più di un milione di sensori attivi in tutto il mondo. I visitatori possono personalizzare la ricerca attraverso diversi parametri,

selezionando i dati secondo i trend delle minacce, le fonti, o focalizzare l'analisi su una determinata regione del mondo. Altra sezione riguarda la "Security Education": un'unica risorsa dà accesso alle best practice del settore, white paper e seminari online. I visitatori, inoltre, possono testare e incrementare la propria conoscenza nel campo della sicurezza informatica grazie a giochi e quiz, accedere al security blog e partecipare a webinar. Per collegarsi e consultare il portale: <http://www.sonicwall.com/securityportal>



LA SICUREZZA AZIENDALE E CONTINUITA' DEL BUSINESS

È disponibile il libro **“Sicurezza aziendale e continuità del business”** realizzato da Reportec.

In circa 350 pagine analizza le problematiche di governance e di risk management connesse con i diversi aspetti della sicurezza aziendale: dalla protezione delle informazioni, alla continuità operativa, alla salvaguardia degli asset fisici, non dimenticando di sottolineare le problematiche portate dagli ultimi trend tecnologici, come il cloud computing e la mobility.

Sono tutti elementi connessi con le minacce che alimentano il rischio: spionaggio industriale, sabotaggi, infedeltà dei dipendenti, incendi e altri tipi di incidenti. Questo libro tratta tali temi considerando che il primo problema da affrontare è di tipo organizzativo e il secondo è di mantenere sempre il controllo degli investimenti in chiave di business.

Completa il volume l'analisi delle soluzioni sviluppate per la sicurezza e la continuità del business da parte un ampio numero di primarie aziende del settore.

Il volume è uno strumento unico in Italia per l'ampiezza delle tematiche affrontate e l'opera di sintesi delle soluzioni e dei servizi disponibili sul territorio, consentendo di approfondire gli aspetti strategici, bilanciando i concetti e la teoria con quanto di concreto attualmente esiste.

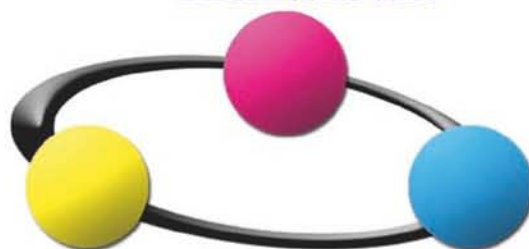
Conoscere è infatti la condizione sine qua non perché un manager possa decidere. Questo obiettivo è perseguito mediante un esame analitico degli aspetti più importanti, gli economics e le modalità di realizzazione e di adozione di una infrastruttura per la sicurezza.

Per acquistarlo manda una mail a info@reportec.it oppure telefona allo **02-36580441**



SECURITY

TECHNOLOGIES



MANAGEMENT

COMPLIANCE

SUMMIT

Edizione 2013

Milano 12-13-14 marzo 2013

Bari 16 aprile 2013 **nuovo**

Roma 5-6 giugno 2013

Verona 3 ottobre 2013



www.securitysummit.it
Per informazioni: CEventi, tel. 02 67101088