

SPECIALE RISK MANAGEMENT E INCIDENT RESPONSE

Dalla valutazione tecnica del rischio alla sua gestione e mitigazione in ottica di business, ritornando al futuro

pag. 12

DOV'È IL CISO?

Da Aipsi considerazioni sull'evoluzione nella gestione della sicurezza alla luce dei nuovi regolamenti che prevedono ruoli e responsabilità

pag. 4



SOLUZIONI

LE SOLUZIONI HPE PER LA PROTEZIONE DELL'AZIENDA DIGITALE

La protezione dell'azienda digitale con l'approccio intelligente e integrato alla security, proposto da HPE per difendere gli utenti, rendere sicure le applicazioni e proteggere i dati

pag. 18

IN QUESTO NUMERO:

AIPSI

pag. 04-08

- Ma dov'è il CISO?

CYBER ATTACK

pag. 09

- Un nuovo malware ogni 4,2 secondi secondo G Data

SPECIALE

pag. 12

- Risk management e Incident response

pag. 14

- Il trasferimento del rischio informatico alle assicurazioni

SOLUZIONI

pag. 18

- Le soluzioni HPE per la protezione dell'azienda digitale

SICUREZZA CHE ESALTA

**ORA PUOI ELIMINARE
MINACCE E COLLI DI BOTTIGLIA.**

La sicurezza Fortinet nasce dalla tecnologia più avanzata
che spiazza concorrenti e criminali.

Ora puoi avere una sicurezza costante
senza mettere a rischio le prestazioni della tua rete.

Visita www.fortinet.it per maggiori informazioni.

FORTINET®

Sicurezza senza compromessi

LA GESTIONE DELLA SICUREZZA, NUOVO "AFFARE" PER IL CISO

La pressione degli attacchi, in particolare verso le grandi imprese, ha raggiunto livelli tali per cui non è più possibile adottare la strategia dello "struzzo", come troppi manager e imprenditori fanno da anni.

Le cronache fungono da campanello d'allarme, ma in molte aziende questo suona a vuoto. È invece imprescindibile attivare una strategia di gestione del rischio informatico come per qualsiasi altra tipologia di rischio. Non a caso crescono le esperienze "assicurative", che potrebbero costituire un ombrello importante per chi subisce un attacco. Il problema è che questo non sempre porta a conseguenze prevedibili. La mancanza di casistiche consolidate rende difficile per le compagnie assicurative valutare i parametri di una polizza che preveda anche danni immateriali e, soprattutto, danni digitali.

Basti per tutte una considerazione: il furto di un computer, in quanto bene materiale, è facilmente riconducibile a un danno appunto materiale, ma i dati che su esso risiedono che valore hanno? Che dire poi del semplice furto dei dati da un server. Intanto è improprio parlare di furto, perché i dati continuano a risiedere sul server in questione da dove sono stati semplicemente copiati. Il valore del danno dipende dall'utilizzo che di questi dati sarà fatto.

Nello speciale su questo numero si affronta il tema dell'incident response come chiave nella gestione del rischio e la questione, negli ultimi anni affrontata da analisi e indagini, relativa al trasferimento del rischio a un soggetto terzo.

Molto interessante è la riflessione di Aipsi sul ruolo del CISO, che proprio della gestione del rischio si dovrebbe occupare.

Security & Business 42
marzo 2016

Direttore responsabile:
Gaetano Di Blasio

In redazione:
Riccardo Florio, Giuseppe
Saccardi, Paola Saccardi

Grafica: Aimone Bolliger

Immagini: dreamstime.com

www.securityebusiness.it

Editore: Reportec srl
Via Marco Aurelio 8
20127 Milano
tel. 02.36580441
Fax 02.36580444
www.reportec.it

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

Tutti i marchi sono
registrati e di proprietà
delle relative società

MA DOV'È IL CISO?

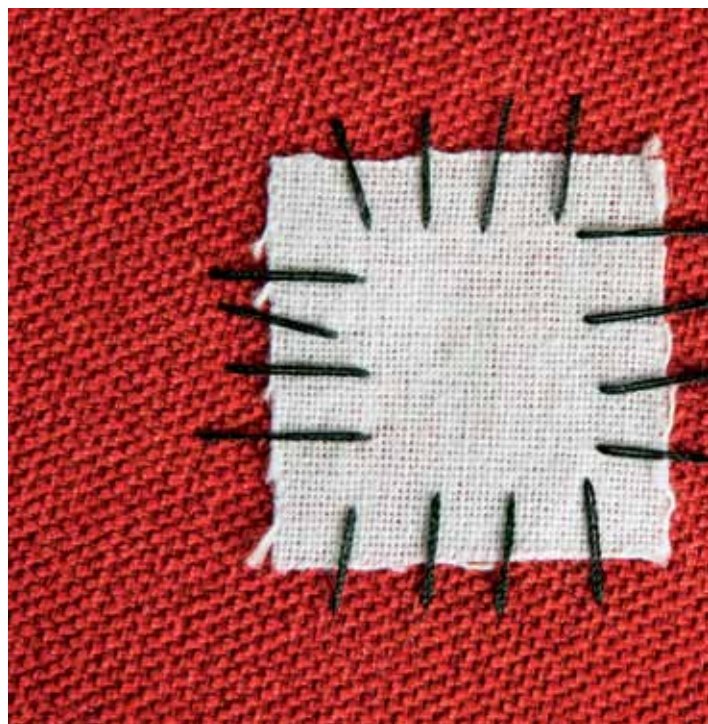
Ruolo e funzione del responsabile della sicurezza digitale nelle aziende ed enti in Italia.

L'aiuto di AIPSI

di Marco Bozzetti

Il ruolo e la funzione di chi si occupa di sicurezza digitale nelle strutture organizzative di enti/aziende in Italia (che nel seguito per brevità verrà indicato con l'acronimo CISO, Chief Information Security Officer) e, più in generale, la struttura organizzativa per la sicurezza digitale, sono un significativo indicatore di come viene percepito, affrontato e governato questo tema, ormai fondamentale per garantire i beni informativi e la continuità operativa dell'intera azienda/ente.

Le competenze richieste a un moderno CISO sono multidisciplinari, da quelle tecniche a quelle manageriali in senso lato, da quelle organizzative a quelle legislative, e richiedono frequenti aggiornamenti. Una figura professionale che ben difficilmente può appartenere, per esempio come dipendente, a piccole e piccolissime aziende/enti lato domanda ICT, che in Italia sono la stragrande maggioranza. Una figura difficile da trovare anche nelle medie e medio grandi organizzazioni, sempre lato domanda ICT. Diversa ovviamente la situazione per le aziende, anche piccole, lato offerta, ossia quelle che operano direttamente nei servizi ICT o che da questi fortemente dipendono.



Dal Rapporto 2016 OAD:

Osservatorio Attacchi Digitali in Italia

I dati del Rapporto 2016 confermano la situazione sopra descritta: il 39,5% ha definito un ruolo di CISO all'interno della propria organizzazione, mentre il 21,7% non lo prevede. Per il 18,6% tale ruolo, pur non definito formalmente, è in pratica attuato dal responsabile dei sistemi informatici (CIO), e per il 17,1% è svolto di fatto da altri ruoli, soventi apicali, quali il responsabile dell'intera azienda/ente (CEO), il responsabile della sicurezza aziendale (CSO), l'ufficio legale, eccetera. Solo una piccola parte del campione dei rispondenti, 3,1%, delega tale ruolo all'esterno a società e/o professionisti di comprovata esperienza.



I rispondenti del rapporto 2016

I rispondenti del Rapporto 2016 appartengono, in termini di dimensioni come numero di dipendenti, al 44% a strutture con meno di 50 dipendenti, al 12,6% a strutture tra i 50 ed i 100 dipendenti, al 10,1% a strutture tra i 101-250, al 12,6% a strutture tra i 251-1000, al 10,9% tra i 1001-5000, al 10,1% oltre i 5001 dipendenti. In termini di settori merceologici di appartenenza, il 22,2% è del settore TLC-Media-Servizi ICT, il 20,9% del manifatturiero, il 20,9% del commercio e servizi (non ICT e banche), il 13,3% della PA, altri settori con % a scendere sotto il 10%.

Fornitori e consulenti

A giudizio dell'autore il su descritto basso valore è anche un indicatore (ma certamente non il solo) della difficoltà, almeno come percezione, di trovare persone e società veramente affidabili, qualificate e competenti in materia.

Nelle piccole e medie strutture lato domanda ICT, le decisioni in merito sono effettuate dalla proprietà e/o dal vertice (il più delle volte coincidono), che, quando succedono problemi (assai rara la prevenzione), si rivolgono ai loro fornitori, tipicamente i venditori del loro hardware e software. Ma questi ultimi sono in grado di risolvere realmente i problemi della sicurezza digitale del loro "piccolo" cliente, o non tendono spesso a piazzare i loro prodotti, vista anche l'incompetenza del compratore?

Il problema è ben noto: etica e competenza del fornitore nei confronti in particolare delle piccole realtà, dove l'ICT, e quindi ancor più la sua sicurezza, è

I dati rilevati dipendono strettamente dal tipo di rispondenti al questionario, sintetizzate nel riquadro: dato il numero non trascurabile in percentuale di aziende lato offerta ICT, la quota di CISO risultante è alta rispetto alla situazione media in Italia. Un elemento di attenzione, stante il campione emerso, è la bassa percentuale di aziende/enti che delegano a terzi la realizzazione e la gestione della sicurezza digitale. Considerando le numerose Pmi rispondenti lato domanda ICT, si sarebbe prevista una percentuale ben maggiore, ben sapendo che le aziende/enti preferiscano di gran lunga gestire all'interno i sempre più critici problemi legati alla sicurezza digitale.

vista solo come una “commodity”, che deve essere economica, veloce da installare e facile da usare. Invece la sicurezza digitale, essendo multidisciplinare e dipendendo molto dal comportamento degli utenti e degli amministratori di sistema, interni o esterni, non è un banale “plug&play”, ma un processo continuo non solo tecnico e che coinvolge tutto il personale dell’azienda/ente, a partire dal vertice. Con il perdurare delle crisi economica e con il mercato in crescita per prodotti e servizi per la sicurezza digitale, è fisiologico che la maggior parte di aziende e di consulenti in ogni branca dell’ICT proclami di essere esperto di sicurezza digitale. Ma la di là del passa parola lato offerta, come è possibile filtrare chi millanta credito da chi ha effettive e buone esperienze?

Certificazioni professionali per la sicurezza e il valore dell'e-CF

Una condizione necessaria ma non sufficiente per un primo filtro è verificare la certificazione dell’azienda e/o dei suoi dipendenti sui più diffusi e consolidati standard e metodiche. Ma ne esistono moltissime sul mercato, in particolare per la sicurezza digitale, da quelle indipendenti come la famiglia ISO 27000, ISO 20000/ITIL, COBIT, CSSP eccetera, a quelle specifiche su prodotti e servizi. Come districarsi da questa giungla di sigle, soprattutto per non esperti ICT? Un significativo aiuto a livello nazionale ed europeo viene dal Decreto. Legislativo. n. 13 del 16 gennaio 2013, da tempo in vigore, sul riordino delle certificazioni con validità legale per le professioni

non regolamentate da Ordini. Tale legge fa esplicitamente riferimento allo standard europeo sulle competenze in ambito ICT, l’e-CF (Competence Framework ripreso - come UNI 11506 a livello italiano e CEN 16234 a livello europeo). Rispetto a tutte le altre certificazioni, il sostanziale valore aggiunto della certificazione e-CF è sintetizzabile nei seguenti punti:

- ha valore giuridico in Italia e in Europa (se erogata da una associazione registrata presso il MISE);
- valorizza le altre certificazioni: averle significa aggiungere punti nella valutazione complessiva;
- si basa sulla provata esperienza maturata sul campo dal professionista;
- qualifica il professionista considerando l’intera sua biografia professionale e le competenze ed esperienze maturate nella sua vita professionale (e non solo per aver seguito un corso e superato un esame).

Due i profili professionali e-CF relativi alla sicurezza digitale, volutamente definiti con un ampio spettro di competenze a più livelli di approfondimento ed esperienza sul campo, come evidenziato nella Tabella:

ICT Security Manager: ruolo di gestore della sicurezza digitale, in pratica il ruolo del CISO

ICT Security Specialist: ruolo di specialista della sicurezza digitale, tipico di consulente interno o esterno e/o di specialista in una delle tante branche della sicurezza digitale.

Per i dettagli sui profili e sulle competenze si rimanda a: <http://www.aicanet.it/e-cf-competenze>.

Le 40 macro-competenze di e-CF, ciascuna articolata su una scala di 5 “qualifiche” (e1-e5) compatibili con l’European Qualification Framework. In rosso sono evidenziate quelle più significative per la sicurezza digitale.

Dimension 1 5 e-CF areas (A – E)	Dimension 2 40 e-Competences identified	Dimension 3 e-Competence proficiency levels e-1 to e-5, related to EQF levels 3–8				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. IS and Business Strategy Alignment					
	A.2. Service Level Management					
	A.3. Business Plan Development					
	A.4. Product/Service Planning					
	A.5. Architecture Design					
	A.6. Application Design					
	A.7. Technology Trend Monitoring					
	A.8. Sustainable Development					
	A.9. Innovating					
B. BUILD	B.1. Application Development					
	B.2. Component Integration					
	B.3. Testing					
	B.4. Solution Deployment					
	B.5. Documentation Production					
	B.6. Systems Engineering					
C. RUN	C.1. User Support					
	C.2. Change Support					
	C.3. Service Delivery					
	C.4. Problem Management					
D. ENABLE	D.1. Information Security Strategy Development					
	D.2. ICT Quality Strategy Development					
	D.3. Education and Training Provision					
	D.4. Purchasing					
	D.5. Sales Proposal Development					
	D.6. Channel Management					
	D.7. Sales Management					
	D.8. Contract Management					
	D.9. Personnel Development					
	D.10. Information and Knowledge Management					
	D.11. Needs Identification					
	D.12. Digital Marketing					
E. MANAGE	E.1. Forecast Development					
	E.2. Project and Portfolio Management					
	E.3. Risk Management					
	E.4. Relationship Management					
	E.5. Process Improvement					
	E.6. ICT Quality Management					
	E.7. Business Change Management					
	E.8. Information Security Management					
	E.9. IS Governance					

L'aiuto di AIPSI

ai professionisti e alle imprese

AIPSI, quale libera associazione a livello personale (non possono aderirvi aziende/enti) di chi a vario titolo si occupa professionalmente di sicurezza digitale, è in grado di aiutare sia i professionisti suoi soci sia le aziende/enti che cercano qualificati professionisti:

A livello dei professionisti AIPSI, anche come Capitolo Italiano di ISSA (www.issa.org) fornisce in maniera continua un trasferimento di conoscenze e di competenze tramite workshop, convegni, corsi di formazione, la rivista ISSA Journal.

A livello di aziende/enti interessate sia lato domanda che offerta ICT

fornisce un punto di incontro tra domanda e l'offerta costituita dalla professionalità dei propri soci operanti sull'intero territorio italiano. Sarà disponibile una specifica area sul nuovo sito Web ora in costruzione, momentaneamente è disponibile uno specifico indirizzo email cui richiedere competenze professionali: domandajob@aipsi.org.

AIPSI promuove la sponsorship a eventi, con argomenti che possono essere concordati con lo (o gli) sponsor e realizza autorevoli eventi di informazione e formazione multi o mono-cliente, totalmente indipendenti da fornitori e produttori, che possono essere specifici sui temi richiesti e svolti sia in aula sia con webinar/e-learning.

AIPSI collabora poi da tempo con AICA per la definizione e l'aggiornamento delle singole competenze atomiche dell'e-CF inerenti la sicurezza digitale,

oltre che a promuovere presso i propri Soci e simpatizzanti le certificazioni e-CF, supportandoli in vario modo per il loro conseguimento.

Il rapporto OAD

Il Rapporto OAD è un'indagine via Web totalmente indipendente e anonimo, sotto l'egida di AIPSI e con la collaborazione della Polizia Postale, cui liberamente rispondono i diversi interlocutori: come indagine via web il Rapporto annuale non ha stretta validità statistica ma, dato il numero di rispondenti e la loro distribuzione tra i diversi settori merceologici e le dimensioni aziendali, fornisce chiare e valide indicazioni sulla situazione e sui trend degli attacchi digitali avvenuti in Italia, e quali sono gli strumenti tecnici e organizzativi di difesa.

I rispondenti del Rapporto 2016 appartengono, in termini di dimensioni come numero di dipendenti, al 44% a strutture con meno di 50 dipendenti, al 12,6% a strutture tra i 50 e i 100 dipendenti, al 10,1% a strutture tra i 101-250, al 12,6% a strutture tra i 251-1000, al 10,9% tra i 1001-5000, al 10,1% oltre i 5001 dipendenti. In termini di settori merceologici di appartenenza, il 22,2% è del settore TLC-Media-Servizi ICT, il 20,9% del manifatturiero, il 20,9% del commercio e servizi (non ICT e banche), il 13,3% della PA, altri settori con % a scendere sotto il 10%.

UN NUOVO MALWARE OGNI 4,2 SECONDI SECONDO G DATA

Nella sua analisi trimestrale G Data ha presentato i dati sul malware e i tipi di attacco più diffusi. In crescita ransomware e adware, concentrati su Windows

di Giuseppe Saccardi

Al peggio non c'è mai fine, recita un vecchio adetto ma sempre attuale, ed è quello che sembra riservare il mondo della sicurezza per quanto riguarda gli attacchi perpetrati e la loro crescente sofisticatezza.

Un'analisi della situazione l'ha condotta G Data, società che produce soluzioni software antivirus. I dati parlano da soli. Nel 2016 l'azienda ha comunicato di aver rilevato quasi sette milioni di nuovi ceppi di malware per workstation, con un incremento del 33% rispetto all'anno precedente. È peraltro un trend che a tutta evidenza non mostra di voler rallentare nemmeno per l'anno in corso perché nel solo primo trimestre la società specializzata nella sicurezza ha già registrato oltre 1.850.000 nuovi tipi di applicazioni malevole.

Ciò corrisponde a un nuovo campione di malware sul mercato (si fa per dire) ogni 4,2 secondi, un valore che supera del 72,6% le rilevazioni degli analisti della società nel medesimo periodo del 2016 e i suoi esperti di sicurezza pronosticano per quello incorso un nuovo record negativo di 7,41 milioni di nuovi malware.

Il tipo di attacco più diffuso

Ma tra tutti quelli emersi quale è il modo maggiormente utilizzato dagli hacker per portare i loro attacchi e dai quali è più urgente difendersi? A conti fatti la quota predominante dei programmi malevoli consta, riporta G Data, di cavalli di troia prodotti tipicamente allo scopo di scaricare ulteriore malware, rilevare i caratteri digitati sulla tastiera, trafugare password o integrare la macchina infetta in botnet per la conduzione di attacchi DDoS.

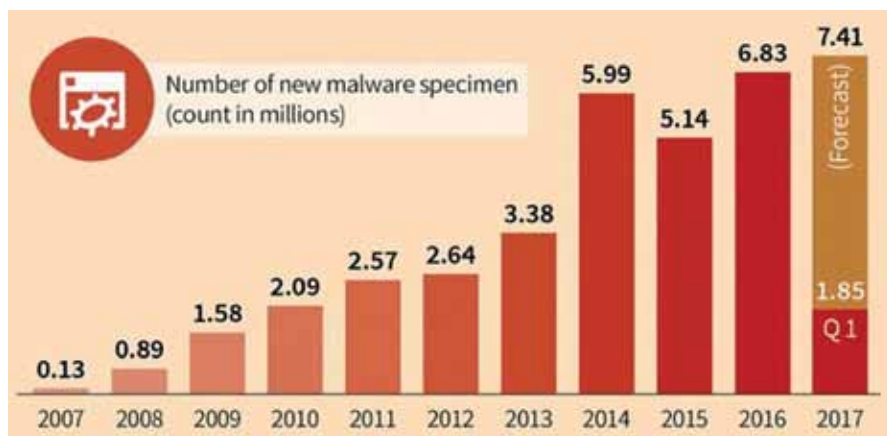
Al secondo posto in classifica figura invece l'adware, che lo scorso anno ammontava a poco meno del 5% delle rilevazioni totali ma già nel primo trimestre

2017 è passato a totalizzare quasi il 14% del malware registrato.

Una citazione si è meritato anche il ransomware, decisamente uno degli attacchi più detestati, anch'esso aumentato in modo più che significativo. Tra il primo e il secondo semestre 2016 era già aumentato quasi di un ordine di grandezza e nel corso del primo trimestre 2017 ha già quasi raggiunto i valori registrati nell'intera seconda metà dello scorso anno.



Ralf Benz Müller, Direttore dei G Data SecurityLabs



Le valutazioni degli esperti sui diversi tipi di attacco si prestano però a interpretazioni diverse quando si parla di realtà oggettiva o di sensazione valutabili «il ransomware ha cagionato danni ingenti destando un notevole interesse

WATCHGUARD INTERNET SECURITY REPORT

Le ricerche del Threat Lab WatchGuard basate sui dati provenienti dalle appliance UTM WatchGuard attive nel mondo

di Giuseppe Saccardi



Il report relativo all'ultimo trimestre 2016 mostra che gli attacchi ransomware sferrati attraverso email di phishing e siti malevoli hanno dominato i titoli dei media, le banche e le organizzazioni sanitarie sono state prese di con esiti sempre più devastanti, e le diverse nazioni hanno continuato a colpirsi a vicenda con attacchi informatici sofisticati. Quanto riportato nel report di WatchGuard in termini di tendenze, statistiche, consigli, vuole essere un aiuto, ha osservato la società, per le aziende a restare aggiornate e attente in un panorama delle minacce molto dinamico e di certo non in senso benevolo.

Cinque i punti salienti che emergono dal report: Circa il 30% del malware è stato classificato come nuovo o "zero-day" poiché non è stato rilevato da una soluzione tradizionale antivirus. Ciò conferma

su scala globale, ma la quota di questo tipo di malware rispetto al totale non è quasi misurabile. L'adware invece è una delle categorie di malware più produttive, ma non viene quasi percepito dagli utenti», ha osservato Ralf Benz Müller, direttore dei G Data SecurityLabs.

In ogni caso, adware o ransomware che sia, una cosa emerge evidente: la parte preponderante dei malware per workstation mira a piattaforme Windows, obiettivo del 99,1% delle applicazioni malevole rilevate. Seguono, sebbene a lunga distanza, script, java applets e macro.

che le capacità dei cybercriminali di riprogrammare in modo automatico o modificare il loro malware ha superato la capacità dell'industria antivirus di tenere il passo con le nuove firme. Senza una soluzione di prevenzione avanzata dalle minacce, capace di identificare in modo proattivo il malware usando tecniche di rilevazione moderne, le aziende non sono in grado di rilevare quasi un terzo del malware. Vecchie minacce diventano ancora nuove. In primo luogo, il malware basato su macro è ancora prevalente. Nonostante sia un vecchio trucco, molti tentativi di spear-phishing includono ancora documenti con macro malevole, e gli attaccanti hanno adattato i loro stratagemmi per includere il nuovo formato di documento di Microsoft. In secondo luogo, gli attaccanti usano ancora shell web malevole per dirottare server web. Shell PHP sono vive e vegete, poiché attaccanti sponsorizzati da Stati hanno fatto evolvere questa vecchia tecnica di attacco con nuovi metodi di offuscamento.

JavaScript è un meccanismo popolare di offuscamento e rilascio del malware. Firebox Feed ha rilevato una crescita in JavaScript malevolo, sia nelle email che sul web.

La maggior parte degli attacchi di rete prendono di mira servizi web e browser. Il 73% dei maggiori attacchi colpisce browser web tramite attacchi drive-by download.

Il principale attacco di rete, Wscript.shell Remote Code Execution, ha quasi interamente colpito solo la Germania. Infatti, scomponendo il dato paese per paese, risulta che l'attacco ha colpito la Germania per il 99% del tempo.

«Il nostro Threat Lab ha monitorato le principali minacce e i trend della sicurezza per anni e ora con l'aggiunta di Firebox Feed - l'analitica in forma anonima delle minacce che provengono dai Firebox WatchGuard implementati nel mondo - otteniamo approfondimenti puntuali e precisi sull'evoluzione degli attacchi informatici e su come gli autori delle minacce si stanno muovendo. Ogni quarter, il nostro report combinerà i nuovi dati provenienti dai Firebox Feed con le ricerche originali e le analisi dei principali eventi di sicurezza per rivelare i trend prevalenti delle minacce e fornire le best practise per la difesa», ha commentato Corey Nacheiner, Chief Technology Officer di WatchGuard Technologies.

RISK MANAGEMENT E INCIDENT RESPONSE

Dalla valutazione tecnica del rischio alla sua gestione e mitigazione in ottica di business, ritornando al futuro

di Gaetano Di Blasio

Partendo dal presupposto che la sicurezza informatica assoluta non è raggiungibile, in passato si è affermata una strategia basata sul risk assessment, in base alla quale le maggiori risorse per la protezione dei sistemi informatici e dei dati devono essere destinate alle aree più a rischio, in quanto punti deboli.

Un approccio "tecnico" che ha presto mostrato i propri limiti. Si è così cominciato a costruire un dialogo tra il dipartimento di informatica e le figure di business dipartimentali, con l'obiettivo di capire quali fossero i processi aziendali più critici e stabilire delle priorità non più in base alle problematiche tecniche, ma all'importanza e all'impatto dei diversi servizi ICT per il business.

Aver spostato l'attenzione direttamente sulle attività principali dell'azienda è quanto di buono resta di questo approccio che è diventato obsoleto con l'evoluzione delle minacce informatiche. Si tratta, infatti, di una strategia ancorata alla vecchia organizzazione a silos dei sistemi informativi, cui corrisponde un modello di protezione altrettanto frammentato e basato sul concetto di perimetro. Comprendendo che il principale punto debole è rappresentato dal fattore umano si è intensificato lo sforzo "educativo"

sul personale aziendale: elemento fondamentale ma insufficiente.

Oggi, con la digital transformation che sta cancellando i confini aziendali e l'utilizzo di dispositivi mobili sempre meno controllabili, si deve adottare un approccio alla sicurezza di tipo integrato e basato su funzioni di intelligence.

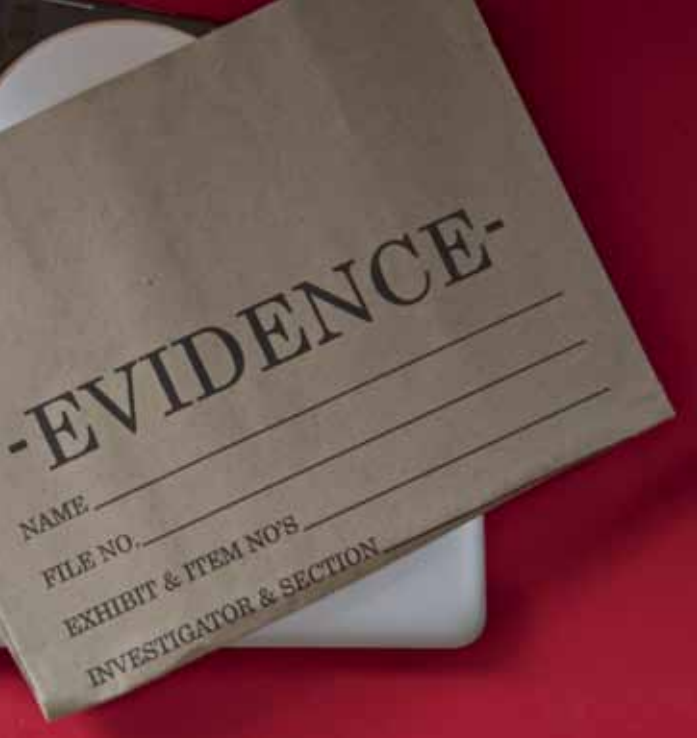
Ancor di più, però, occorre prendere coscienza che, oltre a non esistere la sicurezza assoluta, la probabilità di essere attaccati è 1 in termini statistici, cioè una certezza. Magari è già avvenuto e semplicemente non ce ne si è ancora accorti.

Ritorno al futuro con l'incident response

Dando dunque per scontato che si subirà un attacco, la strategia più opportuna deve salvaguardare l'operatività dell'azienda e basarsi su un piano di risposta agli incidenti che minimizzi il più possibile i danni. Si torna, dunque, a concentrarsi sugli asset più importanti, ottimizzando le risorse nell'ottica della resilienza: piegarsì ma non spezzarsi.

Diverse ricerche (per esempio presso il Ponemon





Institute) hanno dimostrato che le imprese dotate di un team per l'incident response riducono i costi in caso di un attacco andato malauguratamente a buon fine. Un investimento che difficilmente un consiglio di amministrazione può approvare se presentato in questi termini. Quanto sarebbe giusto investire, infatti, non è quantificabile se non è possibile valutare quale potrebbe essere l'ammontare del danno da mitigare.

Tornando al futuro occorre perciò migliorare le pratiche di assessment del passato, per coinvolgere maggiormente il business nella valutazione della sicurezza utilizzando un linguaggio più "economico". Pamela Pace e Alessio Pennasilico, rispettivamente amministratore unico e Security Evangelist di Objective Technology, suggeriscono una quantificazione economica nel Focus "Cyber Risk Management" pubblicato nel Rapporto Clusit 2017.

La loro premessa è: "Un processo di cyber risk management evoluto è essenziale per la corretta valutazione della redditività delle attività di Business e per assicurare che la struttura tecnologica sia coerente con

gli obiettivi di business. Attività questa che raggiunge la sua massima espressione proprio con l'aggregazione dei processi di gestione del rischio cyber all'interno del Enterprise Risk Management Framework. Solo la più radicata convinzione del top management, che questo passaggio sia necessario, segnerà una svolta epocale nella gestione di questo tema".

Gli autori continuano: "In questo senso un grande aiuto può venire dall'analisi del rischio effettuata in maniera quantitativa. Questa metodologia rivoluziona in maniera radicale la misurazione e la gestione del rischio, poiché attraverso un'analisi profonda, volta a misurare economicamente il singolo rischio in funzione delle caratteristiche specifiche di ogni realtà, permette di definire le più opportune strategie di mitigazione in funzione al rischio correlato. Inoltre utilizzando un linguaggio comune a tutti i livelli aziendali, determinato dalla valorizzazione economica dei singoli rischi, renderà possibile una più facile condivisione di questi scenari con il top management, dando di fatto, operativa ancor prima che formale, integrazione del cyber risk all'interno dell'enterprise risk management framework".

Per il successo di questa strategia è fondamentale il ruolo del responsabile dei sistemi informativi, che dovranno imparare a rappresentare il rischio in termini quantitativi: in pratica abbandonando la generica valutazione "rischio alto" con abbinato un codice colorato che da un'indicazione di facile comprensione, ma sostanzialmente poco efficace, per esprimere un valore in "valuta sonante". In questo modo è più semplice per un consiglio di amministrazione considerare degli investimenti, per esempio in un team di incident response o in sistemi per la protezione e, in ultimo, per discutere e valutare un piano assicurativo.

IL TRASFERIMENTO DEL RISCHIO INFORMATICO ALLE ASSICURAZIONI

Aumentano gli sforzi per definire un approccio assicurativo che consideri le peculiarità dei danni da attacco cyber. Il ruolo del Cio.

di Gaetano Di Blasio

Stipulare una polizza assicurativa per tutelarsi in caso di incidenti è una pratica comune. Ma, nel caso di un incidente informatico o, più precisamente, di una violazione alla sicurezza dei dati, non è possibile ricorrere allo strumento assicurativo per mitigare il rischio.

Di fatto le assicurazioni adottano pratiche che possono contare su dati storici e statistiche consolidate, ma la storia del crimine informatico è troppo recente. Inoltre, esiste una differenza importante tra assicurare un bene materiale e uno immateriale. Una cosa è stimare i beni conservati in un "warehouse" (magazzino in inglese), altra è valutare il valore del contenuto di un datawarehouse. Altra ancora è calcolare l'impatto sul business aziendale di una violazione dei dati, che può consistere nella riservatezza, l'integrità o la disponibilità degli stessi.

Ciononostante, esistono alcune forme assicurative, molto differenti tra loro, che sono state illustrate a grandi linee nel rapporto Clusit 2016 e più precisamente in un focus a cura di Alessio Pennasilico, Security Evangelist in Obiettivo, Cesare Burei, amministratore di Margas srl - Consulenti e Broker Assicurativi e Riccardo Scalici, Senior Underwriter



- Cyber Unit – presso Chubb.

Gli autori, sottolineando la scarsità in Italia di polizze legate al mondo informatico, sottolineavano come queste si soffermassero su temi quali:

- danni occorsi ai beni ICT (macchine) e ai dati propri o di terzi;
 - danni legati alla violazione della Privacy (dati personali e/o commerciali) propria o di terzi;
 - danni causati dal crimine informatico e quelli da guasto ed errore umano (di dipendente o terzi);
- danni che impattano sull'attività aziendale (interruzione di esercizio, richieste di risarcimento da parte di terzi).

Balza agli occhi, che parte di queste casistiche è spesso coperta dalle polizze tradizionali, che coprono i danni agli asset aziendali. Occorre, pertanto, considerare con attenzione quali siano i rischi da assicurare che non siano già inclusi in altre polizze, ma per questo, è necessario fare un passo indietro e soffermarsi sugli aspetti basilari del processo che può portare alla stipula di un contratto di una

assicurazione sul rischio cyber security, a cominciare dalla necessità di calcolare i rischi informatici in termini economici.

Per questo, gli autori del focus nel 2016 mettevano in guardia: "conoscere le ratio, i contratti e gli algoritmi utilizzati dalle assicurazioni diventa fondamentale. Quasi tutte le aziende posseggono una polizza incendio. Se a bruciare, però, è la sala server, vedersi rifondere il mero valore dell'hardware sarebbe ottenere un indennizzo sul danno subito più lieve. E come assicurare un furto di dati? Come stimare la differenza tra dati finiti in mano ad un concorrente e dati pubblicati su Internet, come sempre più spesso accade? E un attacco DDoS al proprio sito come si assicura?"

Un team per l'assicurazione cyber

Il GDPR (General Data Protection Regulation) varato dall'Unione Europea, che entrerà in vigore nel maggio 2018, prevede la figura del data officer, che sarà, probabilmente, destinato a valutare il cyber risk e, quindi, ad assumere un ruolo chiave nella stipula di eventuali polizze assicurative.

La mancanza di competenze sul mercato lascia qualche dubbio su come le aziende saranno in grado di organizzarsi e il dubbio su come possa essere affrontata la questione assicurativa.

Burei, in un nuovo focus contenuto nel rapporto Clusit 2017, fornisce una risposta: il cyber risk va affidato a "un tavolo collaborativo che ha nel CIO il suo volano".

È infatti questo il "risponso" contenuto nel white paper "Enterprise Cyber Risk Exposure & Insurance" pubblicato a fine 2016 da Via Virtuosa in collaborazione con Margas e frutto del confronto quotidiano tra le aziende, i broker assicurativi e i consulenti ICT per quasi un anno.

I primi elementi evidenziati dimostrano

che la consapevolezza del rischio cyber e della sua pervasività è aumentata travalicando i confini del tradizionale CED (Centro Elaborazione Dati o EDP – Electronic Data processing), esistendo, ormai,



**SCARICA IL
WHITE PAPER**



un ecosistema digitale fatto di interconnessioni e interdipendenze di processi, persone, macchine e oggetti tra i più disparati.

Viene anche riconosciuto, a più livelli aziendali, che il rischio cyber comprende le conseguenze dirette e indirette di un incidente o attacco. Sottolinea inoltre Burei che si parla sempre più di gestione del rischio in termini di: analisi, mitigazione e trasferimento assicurativo. Sempre l'amministratore di Margas evidenzia che la "business Interruption", la reputazione e la perdita/indisponibilità dei dati sono le maggiori preoccupazioni delle aziende.

Come spiegato da Burei, date le suddette considerazioni, si è deciso di avviare due indagini, poi confluite nel white paper prima citato.

Riportiamo una sintesi di quanto emerso.

La prima indagine, attraverso le risposte di CIO e Amministratori di Sistemi, disegna l'esposizione al rischio da parte delle imprese affinché CFO e CEO possano rendersi conto della centralità dell'attività di Cyber Security gestita internamente o trasferita ai fornitori.

La seconda indagine sempre svolta con l'aiuto del CIO in quanto detentore della dimensione del rischio o dei livelli di protezione messi in atto, cerca di prendere il polso del livello di conoscenza e sensibilità rispetto al tema del trasferimento assicurativo.

I risultati mettono in luce alcuni aspetti che conferiscono al CIO un ruolo chiave nella fase di



**SCARICA
IL WHITE
PAPER**

transizione dalla gestione della ICT security al cyber risk management aziendale di cui il trasferimento assicurativo del cosiddetto "rischio residuo" è una componente ultima, ma fondamentale. Per questo il whitepaper include alcune informazioni di base sul mercato assicurativo italiano e

soprattutto, grazie alle a 18 domande che tre CIO si sono prestati a porre, 18 utili risposte per orientarsi in modo più consapevole nel percorso operativo di acquisizione dello strumento assicurativo.

La certezza di non potersi difendere completamente dal Cyber Risk, impone la sua gestione e una corretta valutazione degli strumenti necessari, del loro costo e dei benefici che questi apportano. In estrema sintesi, è una questione di equilibrio tra l'impatto di un sinistro cyber o cyber-correlato, i soldi investiti nel processo di gestione/ assicurazione e mantenimento delle marginalità aziendali. Afferma Burei: «Quello che è possibile fare è essere proattivi, con investimenti efficaci ed adatti ai rischi aziendali per essere preparati ad affrontare il sinistro e i costi/danni che ne derivano. Le Assicurazioni servono a trasformare un costo/danno incerto e spesso insostenibile in un costo/ premio programmato e sostenibile. La scelta merita una attenta valutazione in fase di prevenzione, affinché effettivamente funzionino da paracadute finanziario ed economico e ci permettano di restare sul mercato evitando la chiusura, perdite bilancio non recuperabili e fornendo gli strumenti per salvaguardare la reputazione del brand».

LE SOLUZIONI HPE PER LA PROTEZIONE DELL'AZIENDA DIGITALE

Il vendor propone un approccio intelligente e integrato alla security, improntato a difendere gli utenti, rendere sicure le applicazioni e proteggere i dati

di Riccardo Florio



Nel 2016 la perdita media per azienda a livello globale è stata di 9,5 milioni di dollari. A sostenerlo è un'indagine promossa da Hewlett Packard Enterprise e realizzata da Ponemon Institute (Cost of Cyber Crime 2016, ottobre 2016) interpellando oltre 1278 professionisti dell'IT e della sicurezza provenienti da 6 Paesi (UK, USA, Giappone, Australia, Brasile, Germania) e operanti all'interno di 237 aziende. Si tratta di una cifra non solo importante (il dato ristretto ai soli Stati Uniti sale a 17 milioni) ma

che cresce rapidamente (+ 23% rispetto al 2015). Per citare un paio di esempi, il costo medio per l'azienda di un attacco Ransomware è di oltre 150mila dollari mentre quello di un incidente legato al furto di credenziali degli utenti è di 232mila dollari.

Dall'analisi di Ponemon emerge che quasi il 40% del danno creato dal cyber crimine è riconducibile alla perdita di informazioni. Inoltre, sono le aziende con una maggiore propensione verso l'innovazione quelle esposte ai maggior rischi: le perdite più ingenti, infatti, sono registrate dalle organizzazioni che hanno effettuato acquisizioni, lanciato nuove applicazioni, sviluppato nuovi prodotti o espanso la loro presenza in nuove aree geografiche.

A questo tipo di rischi HPE pone rimedio attraverso un approccio pensato per costruire la sicurezza partendo dal basso e salendo verso i livelli più alti, focalizzandosi nella protezione delle interazioni tra utenti, applicazioni e dati indipendentemente da dove queste si realizzino.

Il primo passo: prevenire

Prevenire, nella visione di HPE, significa spostare la protezione dal perimetro e portarla più vicina ai

dati stessi. Questo implica utilizzare la crittografia a diversi livelli e concentrarsi sul principale vettore degli attacchi informatici odierni: le applicazioni. Le applicazioni sono intrinsecamente adatte a essere attaccate poiché hanno contribuito progressivamente a fare scomparire il perimetro tradizionale introducendo rischi più sfumati per l'impresa.

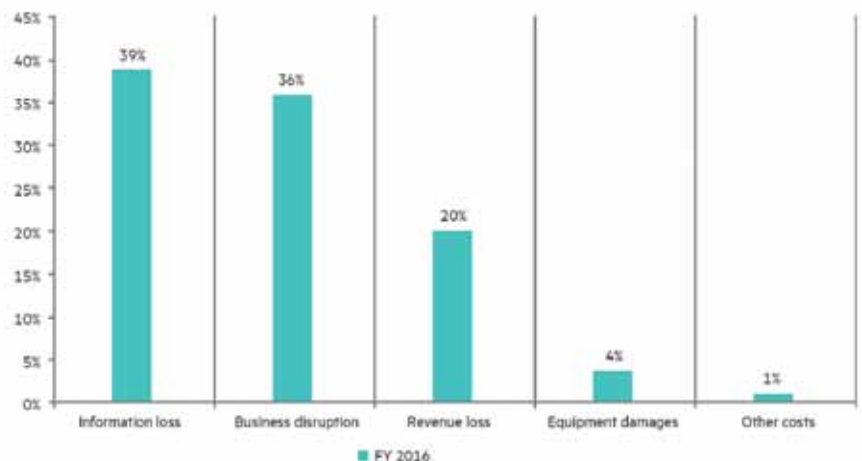
Per garantire la sicurezza delle applicazioni HPE Security persegue una Software Security Assurance ovvero un approccio sistematico e programmatico che si basa sulla ricerca e la riparazione delle vulnerabilità di sicurezza durante l'intero ciclo di vita di un'applicazione. Questo modello si realizza tramite la famiglia di soluzioni HPE Security Fortify che mette a disposizione strumenti per l'esecuzione di test di sicurezza delle applicazioni, funzioni di monitoraggio continuo per la ricerca di vulnerabilità, soluzioni per la gestione della sicurezza del software e l'implementazione di policy di codifica sicure durante lo sviluppo, tecnologie di auto-protezione delle

applicazioni. Sono disponibili anche servizi gestiti per testare la sicurezza delle applicazioni sia in modalità on-premise sia on-demand.

Un ulteriore aspetto che contribuisce alla prevenzione è quello della Data Security, con l'obiettivo di predisporre un livello di protezione che accompagni i dati sempre, sia che si trovino a riposo, in uso o in movimento. In altre parole, invece di focalizzarsi sulle difese perimetrali, HPE Security suggerisce di adottare un approccio di protezione incentrato sui dati che intervenga il più vicino possibile alla fonte stessa dei dati per inibirne l'identificazione e oscurare tutte le informazioni sensibili (come i numeri di conto corrente o di previdenza sociale, le informazioni sulla salute personale o i dati della carta di pagamento). Questi dati protetti possono poi essere trasferiti in sicurezza, utilizzati da altre applicazioni o nei motori di analytics.

Percentage cost by consequence

Consolidated view for six countries



Percentuale di costo del cyber crimine ripartito per categorie di danno

Individuare le minacce e gestire il rischio

Bloccare ogni attacco nell'era della violazione dei dati non è più fattibile. In base a questo presupposto HPE sostiene che, per affrontare realisticamente i problemi di sicurezza odierni, le aziende devono adottare un'ipotesi di compromesso e definire le priorità di rilevamento quando si è verificato un attacco. Ridurre al minimo il tempo di permanenza di un malintenzionato all'interno delle difese aziendali prima di essere individuato è un obiettivo primario per riuscire a limitare i danni arrecati in caso di un attacco andato a buon fine e riuscire a predisporre una risposta efficace.

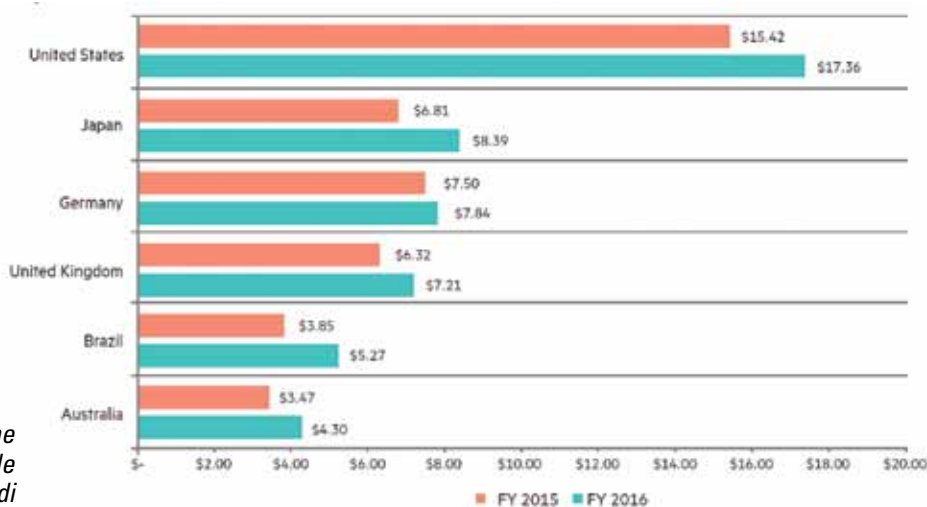
L'uso di strumenti di Security Information and Event Management (SIEM) consente di automatizzare i fondamentali processi di test e avere a disposizione una capacità di analisi per riconoscere le minacce sia note sia sconosciute.

HPE Security offre questa capacità tramite la famiglia di software HPE Security ArcSight. Queste soluzioni realizzano una soluzione SIEM completa in grado di orchestrare e automatizzare i processi di contenimento e risposta alle minacce,

sfruttando tecnologie di analytics di livello avanzato per identificare gli attacchi, gestire i rischi e assicurare la compliance a standard quali PCI, HIPAA, NERC, SOX. HPE Security ArcSight permette di gestire i Big data della sicurezza provenienti dalle più disparate sorgenti (rete, host, applicazioni, utenti), di arricchire i dati con informazioni aggiuntive e di effettuare correlazioni in tempo reale, dimostrandosi efficace anche nella difesa contro le minacce sconosciute o di nuovo tipo come gli APT.

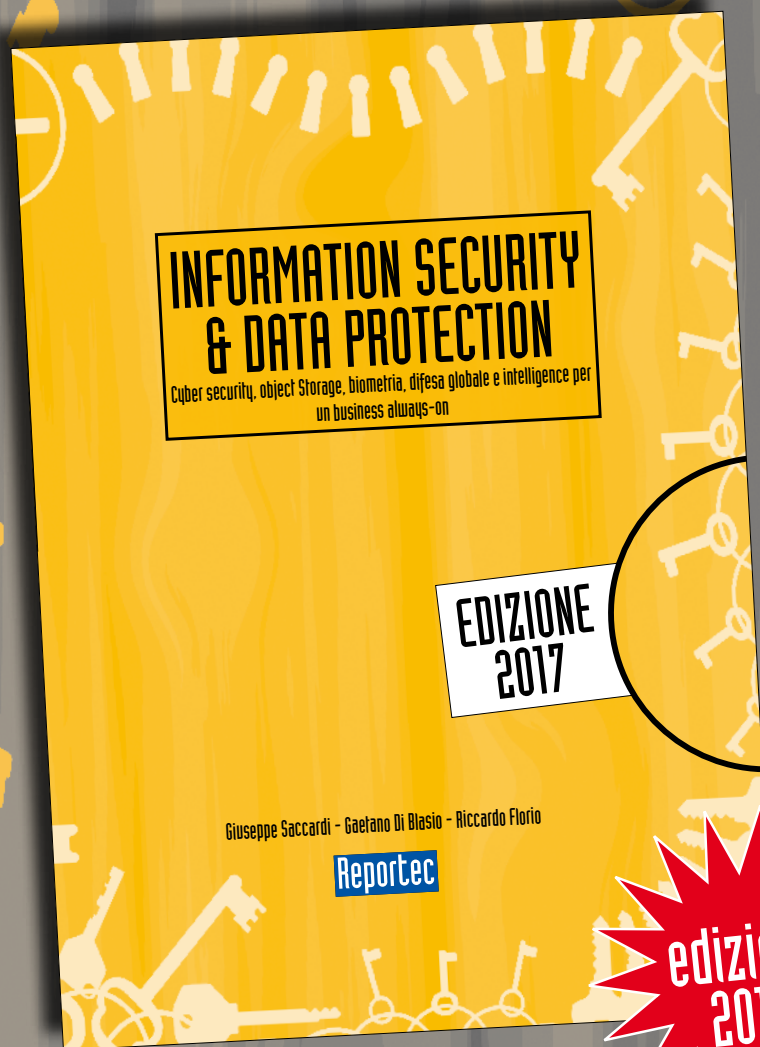
Oltre al software, HPE Security offre altre funzionalità attorno a cui le aziende possono costruire soluzioni di sicurezza che si adattano alle loro specifiche esigenze. In particolare, estendendo le funzionalità di sicurezza con i servizi di sicurezza gestiti, HPE Security aiuta a pianificare, distribuire e ottimizzare la gestione e la governance delle informazioni e predisporre un modello di protezione delle informazioni in grado di estendersi attraverso qualsiasi tecnologia e configurazione.

Costo medio del cyber crimine valutato su 237 aziende campione (dati in milioni di dollari)



Fonte: Ponemon Institute, 2016 Cost of Cyber Crime Study & The Risk of Business Innovation

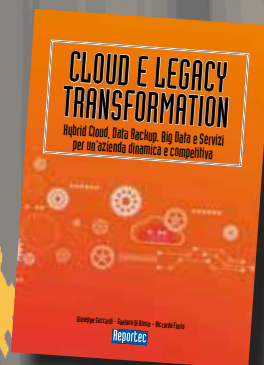
È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**



In oltre 200 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.



È disponibili anche
CLOUD E LEGACY TRANSFORMATION



Il libro è acquistabile al prezzo di 48 euro (più IVA 22%) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444