Anno XV
Gennaio/Febbraio 2016
Poste Italiane S.p.A.
Spedizione in Abbonamento Postale
D.L. 353/03 (Conv. in L. 27/02/2004 n° 46)
Art. 1, Comma 1 – Roma Aut.n C/RM/44/2012
per "ICT SECURITY" id sap 30619433-015
Prezzo € 9,00

ICT Security MAGAZINE

2016 133

www.ictsecuritymagazine.com

- Come gestire la responsabilità della corretta conservazione dei documenti informatici
- La minaccia terroristica alla sicurezza e alle infrastrutture critiche nazionali
- Sicurezza dei dati, tra password e comportamenti
- Cyber Strategy & Policy brief (Gennaio 2016)
- Un anno in retrospettiva: le minacce cyber del 2015
- Il CERT Nazionale

VISITA IL NUOVO SITO DELLA RIVISTA ICT SECURITY

La Rivista inaugura il nuovo sito internet dedicato, veloce e facile da navigare.

NOVITA'
2016

Caratterizzato da un layout moderno, il sito è in grado di garantire un'efficace ed immediata ricerca dei contenuti.

Costantemente aggiornato con le ultime novità del settore e con approfondimenti mirati a fornire al lettore nuovi spunti e linee guida per migliorare ed ampliare il proprio punto di vista rimanendo al passo con la continua innovazione.

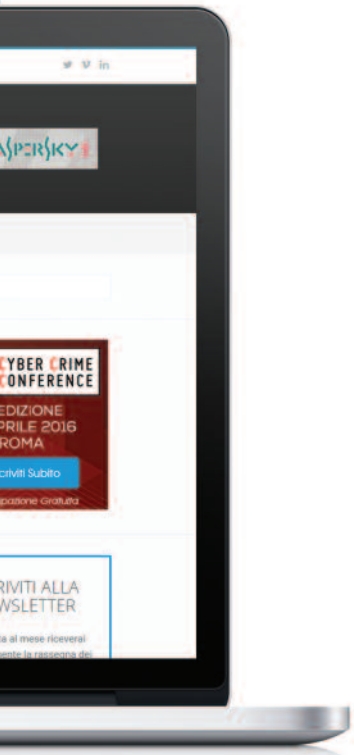
Realizzato per adattarsi automaticamente a tutti i dispositivi di navigazione (pc, tablet, smartphone).

ARTICOLI

NEWS

APPLICATION CASE

INTERVISTE



NEWSLETTER

Iscriviti per ricevere comodamente:

- **Segnalazioni di appuntamenti culturali**
- **Curiosità provenienti dagli specifici mondi**
- **Informazioni editoriali di assoluta attualità**
- **Presentazione in anteprima di nuovi prodotti**
- **Aggiornamenti e offerte riservate**

Vi aspettiamo, quindi, sulle pagine del nuovo sito

www.ICTSecurityMagazine.com

ICT Security

Direttore Scientifico

Corrado Giustozzi

Membro del Permanent Stakeholders' Group di ENISA ed esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT-PA

Coordinamento del Comitato Scientifico

Isabella Corradini

Presidente Centro Ricerche Themis Crime

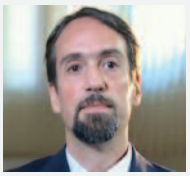
Coordinatore Rubrica
FATTORE UMANO E AMBIENTE DIGITALE

Stefano Mele

of Counsel di Carnelutti Studio Legale Associato e Socio Fondatore di Moire Consulting Group

Coordinatore Rubrica
CYBER SPAZIO E SICUREZZA NAZIONALE

Comitato Scientifico

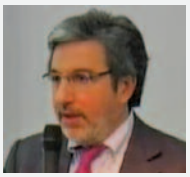


Matteo Cavallini

Responsabile Standard Sicurezza e Sistemi Informativi, Consip

Fabrizio Baiardi

Full Professor Department of Computer Science Università di Pisa



Cosimo Comella

Dirigente Dipartimento tecnologie digitali e sicurezza informatica – Garante per la protezione dei dati personali

Fabrizio D'Amore

Centro di Ricerca di Cyber Intelligence and Information Security (CIS) Università "Sapienza" di Roma

Roberto Di Legami

Direttore del Servizio Polizia Postale e delle Comunicazioni

Rita Forsi

Direttore Generale Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione Ministero dello Sviluppo Economico ISCOM

Luisa Franchina

Presidente di AIIC (Associazione Italiana esperti in Infrastrutture Critiche)

Coordinatore Rubrica
INFRASTRUTTURE CRITICHE

Andrea Lisi

Presidente di ANORC (Associazione Nazionale per Operatori Responsabili della Conservazione digitale)

Coordinatore Rubrica
CONSERVAZIONE, PROTEZIONE E SICUREZZA DEI DATI

Giovanni Manca

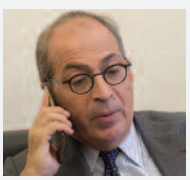
Membro del comitato scientifico di AIFAG (Associazione Italiana Firma Elettronica Avanzata biometrica e Grafometrica)

Coordinatore Rubrica
BIOMETRIA E FIRME ELETTRONICHE

Alberto Manfredi

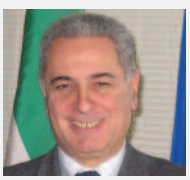
Presidente CSA (Cloud Security Alliance)

Coordinatore Rubrica
CLOUD SECURITY



Paolo Scotto di Castelbianco

Responsabile della comunicazione Istituzionale del Dipartimento delle Informazioni per la Sicurezza della Repubblica, DIS



Domenico Vulpiani

Coordinatore dei sistemi informativi, Ministero dell'Interno

SOMMARIO

COLOPHON

Anno XV - Numero 133 - **Gennaio/Febbraio 2016**

Rivista fondata da
Roberto Scaramuzza

DIRETTORE RESPONSABILE
Riccardo Melito

DIRETTORE EDITORIALE
Edoardo Scaramuzza

PUBLIC RELATIONS MANAGER
Eliana D'Aquanno

SALES AND MARKETING MANAGER
Romina Rakaj

IMPAGINAZIONE
Francesco Tripputi

Finito di stampare nel mese di Febbraio 2016 presso Pixartprinting SpA - Via 1° Maggio, 8 - 30020 Quarto d'Altino VE

ROC - Registro Operatori delle Telecomunicazioni n. 17650 - Pubblicazione mensile registrata presso il Tribunale di Roma n. 113/98 - Tecna Editrice Roma Poste Italiane S.p.A. - Spedizione in Abbonamento Postale - D.L. 353/2003 (Conv. in L. 27/02/2004 n° 46) Art. 1, Comma 1 - DCB Roma

PREZZO DI COPERTINA Euro 9,00
COSTO ARRETRATI Euro 15,00
COSTO ABBONAMENTO PER 9 NUMERI Euro 81,00
da pagare su C/C postale n. 92435809 intestato a Tecna Editrice srl - Viale Adriatico, 147 - Roma 00141

REDAZIONE
Viale Adriatico, 147 - 00141 Roma
Tel. 06 - 871 82 554 - Fax 06 - 81 82 019
E-mail: redazione@tecnaeditrice.com

Riccardo Melito

L'innovazione è ormai tra i pochi strumenti chiave per migliorare i profitti. Con l'evolversi delle tecnologie, soprattutto digitali, un numero maggiore di governi si affida ad essa per migliorare l'economia.
Similmente i nuovi modelli di business si basano sul mutamento tecnologico come unico mezzo in grado di segnare il miglioramento dei processi produttivi creando valori positivi per l'azienda.
Se l'Era Digitale offre innumerevoli opportunità di sviluppo, crescono a ritmo costante anche i rischi e i pericoli che cittadini, imprese ed Istituzioni si trovano a dover affrontare fruendo della rete e dei suoi servizi, con conseguenze non di rado drammatiche per la privacy e la sicurezza dei singoli, per il benessere e la competitività delle aziende, per la salvaguardia delle infrastrutture strategiche su cui poggia il funzionamento di interi Paesi.
Emerge quindi come l'elemento caratterizzante della sicurezza informatica sia l'incertezza.
L'unico strumento per ridurre tale stato di incertezza è il costante aggiornamento, assicurarsi perciò di aver fatto ricorso agli ultimi ritrovati sia metodologici che tecnologici del settore.
Un aggiornamento che deve avvenire giorno dopo giorno. Ed è per questo che la rivista ICT Security, sin dal 2002, è diventata un'utile strumento di consultazione sia per il fornitore di servizi e prodotti della sicurezza sia per il fruitore di tali servizi.
Per raggiungere questi obiettivi abbiamo coinvolto i più qualificati professionisti ed esperti provenienti dal mondo delle istituzioni e delle aziende leader nel settore che illustreranno le principali novità poste dall'evoluzione delle tecnologie legate alla sicurezza informatica secondo un approccio concreto e dinamico che, all'analisi dei problemi, accompagna intelligentemente sempre la ricerca di risposte e soluzioni con pareri e confronti utili ad informare l'utente finale. Verranno quindi affrontati gli aspetti metodologico organizzativi della sicurezza informatica insieme all'innovazione tecnologica.
Questo è il compito che svolgerà il nuovo comitato scientifico composto da autorevoli esperti del settore e diretto da Corrado Giustozzi, Membro del Permanent Stakeholders' Group di ENISA ed esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT-PA e coordinato da Isabella Corradini, Presidente Centro Ricerche Themis Crime, e Stefano Mele, of Counsel di Carnelutti Studio Legale Associato e Socio Fondatore di Moire Consulting Group.
La rivista proporrà contenuti tecnico-scientifici di aggiornamento sull'evoluzione delle tecnologie dell'informazione e della comunicazione capaci di mobilitare l'interesse delle istituzioni, del tessuto economico e della società civile, oltre a quello degli specialisti tramite le seguenti rubriche: Biometria e firme elettroniche, Cloud Security,
Cyber Spazio e Sicurezza Nazionale, Fattore Umano e Ambiente Digitale, Infrastrutture Critiche e Conservazione, Protezione e Sicurezza dei dati.
Ultima novità da segnalare prima di lasciarvi alla lettura è la nascita del sito dedicato alla rivista www.ictsecuritymagazine.com.
Per quanto mi riguarda avrò il compito di introdurvi ad ogni numero. Spero di rendervi la lettura piacevole.

Buona lettura. ■

ABBONAMENTO 2016

SCEGLI LA TUA FORMULA

20% SCONTO

CARTA + DIGITALE

1 ANNO € 64,80
COMPRESO DI SPEDIZIONE

anziché € 81,00
9 numeri

DIGITALE

1 ANNO € 45,40

anziché € 56,70
9 numeri

ICT SECURITY

RIVISTA DEDICATA ALLA SICUREZZA INFORMATICA

La prima pubblicazione italiana dedicata in forma esclusiva alla sicurezza informatica e al business continuity, si pone l'obiettivo di coinvolgere i più importanti attori del settore, Aziende e Istituzioni Pubbliche, per la diffusione degli elementi conoscitivi legati alla sicurezza e ai programmi di eGovernment.

PER ATTIVARE L'ABBONAMENTO VAI SU www.tecnaeditrice.com

PRESENTAZIONE RUBRICA CONSERVAZIONE, PROTEZIONE E SICUREZZA DEI DATI

Andrea Lisi,
Presidente di ANORC

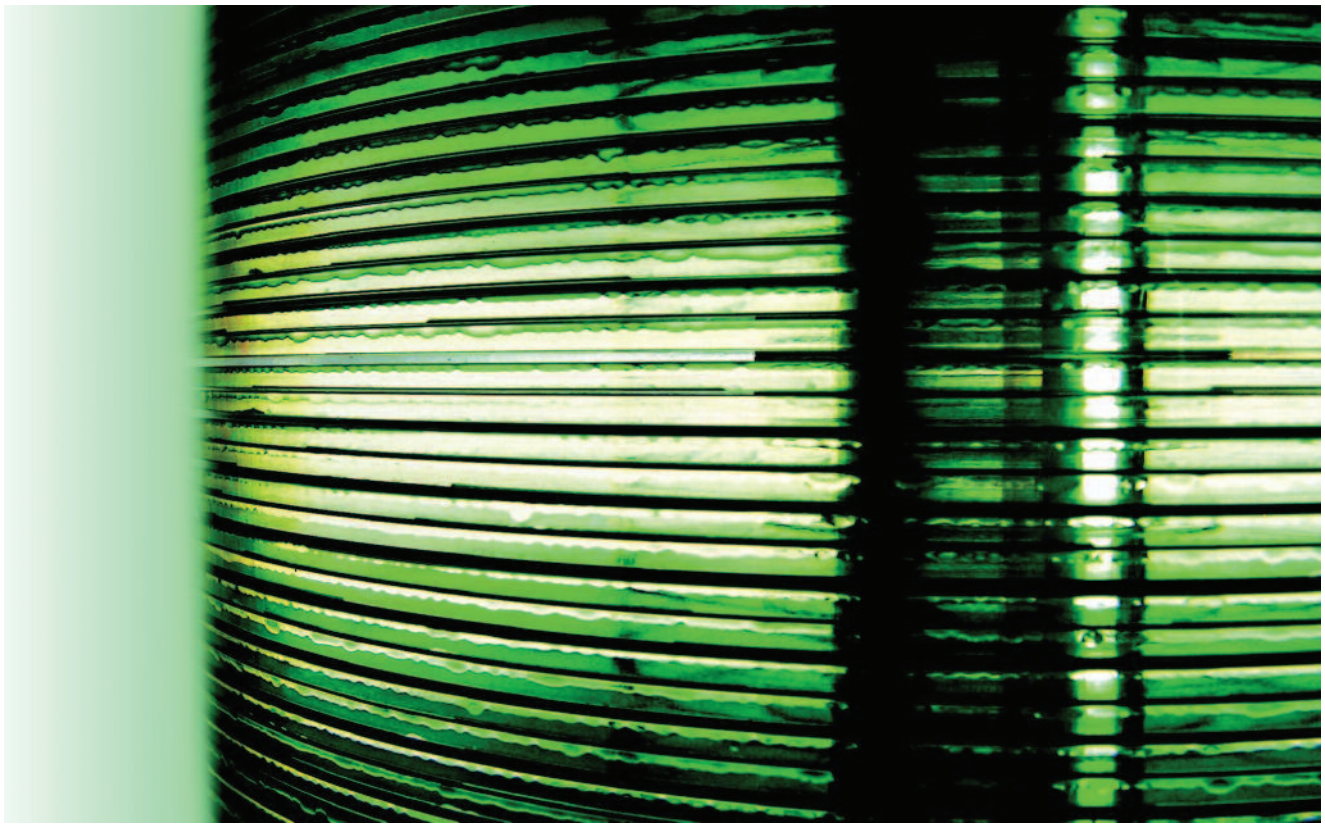
Mentre la Integrated Industry e le aziende 4.0 sono argomenti che occupano sempre più spazio nelle testate di informazione e vengono prospettati spesso come un futuro imminente se non come un presente già in corso, lo scenario reale offerto dalle imprese italiane non è poi così unilateralmente innovativo, soprattutto per quanto riguarda il primo step fondamentale verso l'innovazione che consiste nella gestione digitale, consapevole e sicura, di dati e documenti.
Molte aziende, infatti, adottano ancora un approccio frammentario alla governance delle proprie informazioni rilevanti, con un impatto negativo in termini di efficienza, sostenibilità e sicurezza.
Non si tratta solo della corretta produzione e conservazione dei documenti informatici: la mancanza di un approccio strutturato, infatti, non consente di avere un pieno controllo sui dati e questo rende non solo vulnerabili società, studi professionali e/o PA a violazioni della sicurezza (siano esse accidentali o intenzionali), ma li espone anche a contestazioni in merito all'affidabilità (anche giuridica) del loro patrimonio informatico e documentale.
E le violazioni accidentali al proprio patrimonio di dati non sono da trascurare se da un recente studio elaborato da una società di corporate intelligence è emerso che nel 75% dei casi di violazione dati all'interno dell'azienda il responsabile è un dipendente e ben 6 violazioni su 10 avvengono per sbaglio.
La custodia sicura dei documenti dovrebbe essere garantita in maniera trasversale e coinvolgere l'azienda (o la PA) in ogni suo processo, tenendo conto, inoltre, che ci sono informazioni di cui è necessario, più di altre, garantire la riservatezza, l'integrità, la confidenzialità e la reperibilità.
In questa rubrica che qui inauguriamo, ospitata tra le pagine di ICT Security, cercheremo di affrontare due principali argomenti: come le aziende e le pubbliche amministrazioni gestiscono in modo affidabile la riservatezza e l'autenticità dei documenti informatici e quali possibili rischi si corrono in caso di violazione delle regole tecniche attualmente in vigore.
Senza il rispetto di procedure formali e a norma di legge finalizzate alla sicurezza e alla custodia affidabile dei dati, le

Andrea Lisi: Avvocato esperto in diritto delle nuove tecnologie, Presidente ANORC e ANORC Professioni, Segretario Generale AIFAG e Coordinatore del Digital & Law Department dello Studio Legale Lisi. È Docente presso la Document Management Academy e la MIS Academy della SDA Bocconi.

ANORC
Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale

ANORC: Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti) dal 2007 mette in comunicazione conoscenze e bisogni di aziende, enti pubblici, professionisti ed esperti che operano nella Dematerializzazione e Conservazione digitale, con lo scopo di garantire ai nuovi archivi digitali durata e immutabilità nel tempo. L'associazione promuove attività di studio e formazione sulle tematiche del digitale e sostiene un dialogo attivo con le istituzioni centrali (www.anorc.it).

aziende (e le PA) si espongono a rischi di notevole entità che posso ripercuotersi direttamente sul business (o sull'affidabilità del proprio archivio).
Inoltre, credo che sia opportuno ricordare come la divulgazione non controllata di informazioni che dovrebbero invece rimanere riservate potrebbe vanificare gli investimenti in materia di ricerca e sviluppo, generare una perdita di fiducia da parte dei propri clienti e in ultimo (fatto non meno importante) esporre a pesanti sanzioni.
Essere consapevoli dei vantaggi che derivano da una corretta governance dei propri dati e documenti è, quindi, il primo passo da compiere. Non meno importante sarà individuare in modo chiaro e trasparente le diverse responsabilità legate alla gestione dei flussi di dati e assicurarsi che i propri dipendenti, a maggior ragione coloro che svolgono dei ruoli chiave come il Responsabile della Conservazione e il Responsabile del Trattamento, abbiano una preparazione adeguata alle responsabilità a cui devono far fronte.
L'innovazione digitale ha colto molte organizzazioni alla sprovvista, così in tanti casi si è improvvisato, investendo personale non specializzato di incarichi per svolgere i quali occorre possedere invece una professionalità specifica, con tutti i rischi che ne derivano: è per questo che ANORC e ANORC Professioni, le associazioni che presiedo, stanno conducendo ormai da anni una battaglia per il riconoscimento e la corretta valorizzazione delle competenze specifiche dei professionisti della digitalizzazione e della privacy che operano all'interno di ogni organizzazione - pubblica o privata che sia - insistendo molto sull'importanza della formazione.
Non si tratta di noiosi cavilli burocratici, di regole per gli addetti da rispettare solo superficialmente, ma di fattori chiave che hanno ricadute importanti anche in termini economici.
Le aziende in grado di garantire l'affidabilità dei loro processi di gestione dati, attraverso una giusta organizzazione e l'apporto di personale preparato, posseggono una marcia in più con la quale potranno aumentare il loro vantaggio competitivo e rafforzare la fiducia dei loro clienti. ■



COME GESTIRE LA RESPONSABILITÀ DELLA CORRETTA CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Sarah Ungaro,
Digital&Law Department Studio Legale Lisi – Ufficio di Presidenza ANORC

Per delineare l'assetto di ruoli e responsabilità nelle attività relative alla conservazione dei documenti informatici, occorre innanzitutto chiarire che **tale obbligo dovrà essere assolto dal soggetto che ha prodotto il documento o da colui che, per legge, deve custodirlo**.
In tema di documento informatico, il Codice dell'amministrazione digitale (D.Lgs. n. 82/2005) stabilisce che i documenti degli archivi, le scritture contabili, la corrispondenza e ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, se riprodotti su supporti informatici, sono validi e rilevanti a tutti gli effetti di legge, a patto che la riproduzione e la conservazione nel tempo siano effettuate in modo da garantire la conformità dei documenti agli originali. Inoltre, il CAD dispone che i documenti informatici, di cui è prescritta la conservazione per legge o regolamento, debbano essere conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche. **La responsabilità della conservazione ricade, quindi, direttamente sul soggetto che, per legge o regolamento, è tenuto a garantirla**.
La **responsabilità** del titolare dei documenti informatici sulla corretta conservazione degli stessi è stata **ribadita più volte anche dall'Agenzia delle Entrate**, con specifico riferimento ai documenti fiscalmente rilevanti: nella Risoluzione 161/E del 9 luglio 2007, ad esempio, si è precisato che "*in tutti i casi in cui il contribuente affida, in tutto o in parte, il processo di conservazione a soggetti terzi continuerà a rispondere nei confronti dell'Amministrazione finanziaria della corretta tenuta e conservazione delle scritture contabili e di tutti i documenti fiscalmente rilevanti. Eventuali inadempienze del soggetto incaricato della conservazione non potranno essere opposte all'Amministrazione finanziaria per giustificare irregolarità o errori nella tenuta e nella conservazione della contabilità o, più in generale, di tutti i documenti rilevanti ai fini tributari* [...]".
Pertanto, **il conferimento a terzi dell'incarico di effettuare la conservazione** a norma dell'art. 44 e ss. del CAD **non incide sugli obblighi di corretta tenuta e conservazione** di libri, registri, scritture, fatture e di tutti i documenti prescritti dalla normativa fiscale, **che continuano a gravare sul contribuente**.
Eventuali inadempienze dei suddetti obblighi che diano luogo all'applicazione di sanzioni sono, dunque, addebitate al soggetto tenuto al rispetto delle prescrizioni in materia di corretta gestione e conservazione dei documenti.
Con particolare riguardo al ruolo del Responsabile della conservazione, il Codice dell'amministrazione digitale stabilisce all'art. 44 (commi 1-bis e 1-ter) che "*il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196,* [...]" e che lo stesso "*può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione* [...] *ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche*"[1].

[1] È utile ricordare che secondo l'art. 2 comma 3 del Codice dell'amministrazione digitale queste specifiche disposizioni relative alla conservazione dei documenti informatici si applicano an iche ai privati e non solo alle pubbliche amministrazioni.

La conservazione a norma dei documenti, dunque, **può essere svolta** - sempre sotto la gestione del Responsabile - **o all'interno** della struttura organizzativa del soggetto titolare **o "*affidandola, in modo totale o parziale, ad altri soggetti pubblici o privati*"** che, sulla scorta dell'art. 5 delle Regole tecniche, di cui al DPCM 3 dicembre 2013, offrano idonee garanzie organizzative e tecnologiche, come l'essere accreditati come conservatori presso l'Agenzia per l'Italia digitale.

La gestione, in piena responsabilità e autonomia, **del sistema di conservazione spetta dunque sempre al Responsabile della conservazione**: sia qualora la conservazione venga svolta internamente alla struttura organizzativa del soggetto produttore dei documenti informatici da conservare, sia quando venga affidata, in modo totale o parziale, ad altri soggetti pubblici o privati (Conservatori) che offrano idonee garanzie organizzative e tecnologiche. Vengono così confermate e sottolineate la complessità e la responsabilità connesse a tale ruolo che, **rendendo necessarie varie e differenti competenze (informatiche, giuridiche, archivistiche)**, deve essere affidato a soggetti apicali all'interno della struttura che ha la responsabilità di conservare i documenti informatici prodotti.

È opportuno sottolineare che – come peraltro specificato dall'Agenzia delle Entrate nella Circolare 36/2006 - già dalla sola analisi dell'art. 44 del CAD pare evincersi la "naturale" collocazione del ruolo del Responsabile della conservazione all'interno della struttura organizzativa del titolare dei documenti conservati, o comunque della riferibilità di tale ruolo in seno a un "rapporto qualificato" (un socio, un amministratore, o comunque un soggetto che ricopre una posizione apicale) o comunque di fiducia con la

società, l'associazione o l'ente titolare dei documenti[2] (come, ad esempio, un consulente esterno di fiducia dello stesso soggetto titolare dei documenti, ma tale soluzione è ipotizzabile solo per i soggetti privati)[3].

Diversamente, alla luce dell'assetto di responsabilità delineato dalla normativa, non risulta corretto che il Responsabile della conservazione nominato dal titolare abbia in essere un rapporto di lavoro anche con il soggetto Conservatore esterno, in quanto in tale eventualità potrebbe risultare difficile escludere, in linea generale, la potenziale sussistenza di un **conflitto di interessi** nell'esecuzione dei compiti e delle funzioni del Responsabile della conservazione.

In tal senso, analizzando con attenzione la formulazione letterale e la tecnica normativa con cui sono state redatte le nuove Regole tecniche, è possibile cogliere altri indizi circa la configurazione del ruolo del Responsabile della conservazione. Tale figura, infatti, sempre sotto la propria responsabilità, può delegare lo svolgimento del processo di conservazione o parte di esso, ad altri soggetti di specifica esperienza e competenza. La delega (atto che solitamente prevede l'esistenza di un rapporto strutturato a priori tra il delegante e il delegato) dovrà essere formalizzata indicando tutte le specifiche funzioni e competenze affidate al delegato. **Pur potendo spogliarsi di tutte le funzioni legate al processo di conservazione, quindi, il Responsabile resta comunque responsabile dell'intero processo**.

Anche laddove venga scelto di affidare

[2] O, per riprendere la fattispecie esaminata dalla Agenzia delle Entrate nella Circolare 36/2006, "il contribuente diverso da persona fisica".

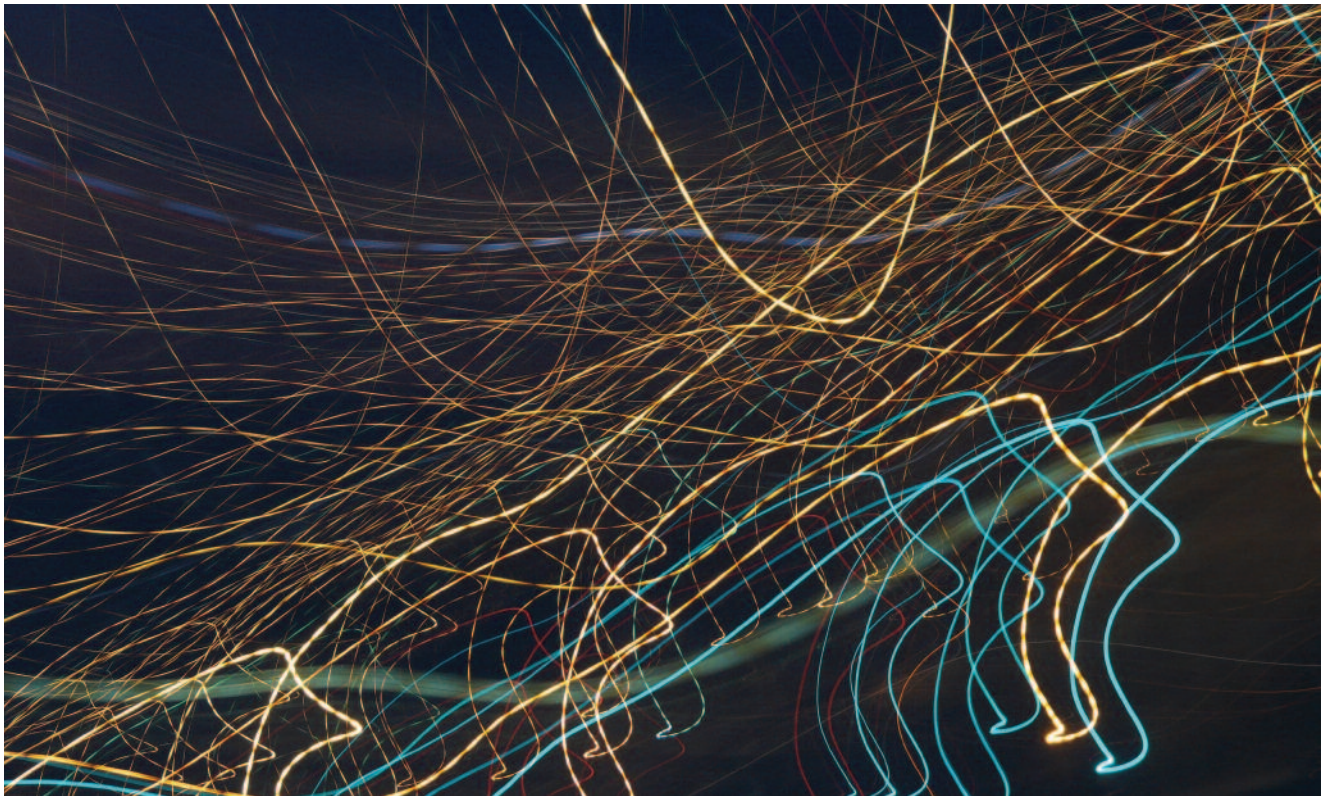
[3] In effetti, la nomina a Responsabile della conservazione di un consulente esterno è in ogni caso da escludersi per le pubbliche amministrazioni alla luce dell'espressa previsione del comma 3 dell'art. 5 delle Regole tecniche di cui al DPCM 3 dicembre 2013, nel quale si stabilisce, ribadendo la delicatezza e la complessità di tale ruolo, che "nelle pubbliche amministrazioni, il ruolo del Responsabile della conservazione è svolto da un dirigente o da un funzionario formalmente designato".

la conservazione all'esterno della struttura, tale affidamento dovrà essere effettuato mediante contratto o convenzione e dovrà prevedere l'obbligo del rispetto del Manuale di conservazione predisposto dal Responsabile. Anche in questo caso, quindi, la norma tecnica dev'essere letta alla luce della normativa primaria che riconosce al Responsabile la possibilità di affidare all'esterno il sistema e, tale affidamento, non permette comunque di spogliarsi della propria responsabilità, quantomeno nei termini di eventuale ***culpa in eligendo*** e ***culpa in vigilando***.

Si sottolinea che con l'introduzione delle Regole tecniche approvate con il DPCM 3 dicembre 2013, sono state specificate le attività di competenza del Responsabile della conservazione, che "*è colui che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato*". Peraltro, le Regole tecniche stabiliscono che tali attività vengano svolte d'intesa con il Responsabile della sicurezza e dei sistemi informativi (oltre che con il Responsabile della gestione documentale, ove nominato).

In effetti, **punto cardine** della trattazione negoziale è anche quello relativo alla **riservatezza dei dati e delle attività svolte dal Conservatore** per l'azienda o l'ente che affida in outsourcing la conservazione: si pensi alla massa di documenti, dati, e informazioni che "migrano" dalla struttura titolare al Conservatore, affinché quest'ultimo possa attuare le operazioni a cui è preposto. Trattandosi poi di attività aventi ad oggetto molto spesso servizi informatici, non trascurabile risulta essere anche l'aspetto della **sicurezza**: il titolare dovrà, in tal senso, imporre al fornitore, laddove già lo stesso non vi abbia espressamente provveduto, l'adozione di misure di sicurezza tali da tutelare l'attività da accessi non autorizzati o manomissioni che comportino conseguenze quali distruzione e perdita dei dati.

Le stesse regole tecniche prevedono, infatti, che il Conservatore esterno assuma *ex lege* il ruolo di Responsabile esterno del trattamento dei dati, così come previsto dal Codice in materia di protezione dei dati personali. ■



PRESENTAZIONE RUBRICA BIOMETRIA E FIRME ELETTRONICHE

Giovanni Manca,
Membro del comitato scientifico di AIFAG

Sono passati esattamente dieci anni (era l'1 gennaio 2006) dall'entrata in vigore del Codice per l'amministrazione digitale, comunemente noto come CAD, a seguito del D. Lgs. n. 82 approvato il 7 marzo dell'anno precedente. Con questo ricordo si apre il 2016 delle sottoscrizioni informatiche anche perché il 1 luglio del 2016 entra in vigore il Regolamento 910/2014 che cambia completamente lo scenario delle firme e di tanti altri servizi connessi all'agenda digitale.
A cambiare, prima di tutto è il glossario, scompare infatti il certificatore accreditato o il gestore di posta elettronica certificata ai quali dovremo riferirci come *prestatori di servizi fiduciari*.
Numerose altre modifiche e innovazioni saranno operative come i servizi di recapito certificato qualificato e i sigilli elettronici.
Tutti questi argomenti saranno trattati nei prossimi numeri con le opportune descrizioni e gli approfondimenti del caso compreso quanto attinente al nuovo Codice dell'amministrazione digitale (CAD) che sarà promulgato in attuazione della Riforma della pubblica amministrazione Italiana.
Il CAD vigente è stato significativamente modificato considerato che le regole nazionali in materia di firme sono completamente in linea con la direttiva 1999/93/CE su un quadro comunitario delle firme elettroniche che sarà abrogata il 1 luglio del 2016 in contemporanea con l'entrata in vigore del Regolamento eldAS.
Per esempio sono state eliminate le definizioni già presenti nel Regolamento in quanto duplicazioni; le procedure di accreditamento dei certificatori lasciano il posto a quelle di qualifica dei prestatori di servizi fiduciari.
Il coordinamento tra la normativa nazionale e quella comunitaria (che essendo Regolamentare è di rango superiore) è stato condotto con l'obiettivo di garantire continuità al mercato nazionale di riferimento, assicurando, contemporaneamente un adeguato equilibrio con i

Giovanni Manca: laureato in Ingegneria Elettronica, svolge attività di consulenza sulle tematiche di dematerializzazione e sicurezza ICT. Da circa 25 anni si occupa di attività tecnologiche nel settore dell'ICT avendo spaziato nel corso degli anni dal network and system management alle infrastrutture a chiave pubblica (PKI).
Ha partecipato alla creazione della prima firma elettronica nella pubblica amministrazione, alla messa in linea del primo sito internet della fiscalità, al primo progetto pubblico di disaster recovery di dati fiscali, alla progettazione della Carta Nazionale dei Servizi e della Carta d'Identità Elettronica. Ha partecipato alla stesura delle più importanti normative tecniche sui temi dell'e-government. Attualmente è senior advisor sulle tematiche di dematerializzazione e sicurezza ICT per alcune primarie società di settore.

AIFAG: Associazione Italiana Firma elettronica Avanzata Biometrica e Grafometrica, promuove e sostiene nel mercato delle firme – caratterizzato ancora da disomogeneità - l'adozione di standard sicuri e interoperabili, inoltre stila e fornisce linee guida e best practice sull'utilizzo corretto della firma elettronica avanzata, biometrica e grafometrica (www.aifag.it).

mercati esteri che emergeranno negli altri Stati membri e che avranno pieno titolo, senza barriere di sorta ad operare nel mercato nazionale.
Ma eIDAS introduce anche elementi con primario valore giuridico che, correttamente, non sono stati inseriti nel CAD perché totalmente innovativi e quindi avremmo una duplicazione di elementi opposta a quella descritta per le definizioni. Cioè sarebbe inutile importare nel CAD quanto stabilito nel Regolamento eIDAS.
Al nuovo CAD si dovranno affiancare rapidamente nuove regole tecniche di settore che tengano in conto gli elementi innovativi introdotti dal Regolamento. Quando tali regole saranno diverse da quelle comunitarie quelle nazionali non potranno essere applicate e soprattutto l'emissione delle regole non è più a carico o sotto il controllo diretto degli Stati membri, ma saranno gli organismi di standardizzazione come ETSI e CEN ad emettere regole e poi la Commissione UE, con il parere degli Stati emetterà provvedimenti denominati atti di esecuzione o atti delegati ai quali i medesimi Stati dovranno attenersi.
Nei prossimi numeri svilupperemo tutte queste tematiche relative alle firme e alle tecnologie indispensabili per la loro corretta realizzazione e diffusione.
Un altro argomento di questa rubrica è la biometria.
Negli ultimi due anni abbiamo assistito ad una vertiginosa diffusione della firma elettronica avanzata basata su tecniche biometriche ovvero alla firma grafometrica. Il Regolamento eIDAS non modifica quanto stabilito dal CAD e dalle specifiche regole tecniche sul tema e questo è un vantaggio per lo sviluppo del mercato grafometrico. Questo è ancora molto scarso nella pubblica amministrazione e nel settore privato diverso da quello bancario/finanziario o assicurativo.
Ci occuperemo quindi dello stato dell'arte, di proposte per l'aggiornamento delle regole tecniche della FEA che in alcuni punti sono obsolete o bloccanti. Un altro interessante argomento da affrontare è quello dell'ipotesi di aggiornamento del fondamentale provvedimento prescrittivo del Garante per la protezione dei dati personali in materia di biometria. Infatti oltre alla grafometrica si stanno diffondendo velocemente altri tipi di applicazioni biometriche a partire dal mondo bancario ma anche nella domotica.
Quindi comincia a essere possibile approcciare l'*internet banking* in chiave totalmente biometrica.
Per effettuare un bonifico quindi, già oggi, non sarebbe fantascienza entrare nel sistema bancario con il proprio volto, dare disposizioni tramite voce e confermare le transazioni tramite l'impronta digitale.
E nemmeno operare nella domotica con il riconoscimento vocale o facciale è già nella disponibilità di mercato e avrà la sua diffusione nei prossimi mesi ed anni.
Il che significa che i paradigmi e gli approcci alla privacy (e non separatamente alla sicurezza) dovranno essere diversi e con il giusto grado di consapevolezza.
Seguiteci e tutti gli argomenti sinteticamente qui anticipati e gli altri che emergeranno dall'evoluzione di queste tematiche saranno trattati ai fini della diffusione dell'informazione e della conoscenza scientifica. ■

PRESENTAZIONE RUBRICA CLOUD SECURITY

Alberto Manfredi,
Presidente CSA

Il Cloud Computing rappresenta oggi il nuovo paradigma verso il quale stanno convergendo tutte le nuove strategie di implementazione di infrastrutture, sviluppo applicazioni e servizi ICT.
La maggior parte delle aziende ICT, in particolar modo le medio-grandi, hanno già trasformato la propria offerta in "cloud services" mentre le start-up nascono immediatamente "cloud-ready". Parallelamente i nuovi approcci e le nuove sfide dell'Information Security hanno superato i confini aziendali, il cosiddetto "perimetro", considerando ormai il dato-informazione come un bene "mobile", disponibile su richiesta, da qualunque rete e qualunque dispositivo di accesso (pc, smartphone, tablet, watch, glass, metering, ...).
Il Cloud Computing è di fatto un paradigma pervasivo e trasversale nell'organizzazione attuale delle aziende, sia fornitori sia utilizzatori, e richiede un processo di formazione ed allineamento continuo tra tutte le parti interessate (stakeholders) nel processo di definizione, acquisto, utilizzo, gestione (governance) e sicurezza di un servizio Cloud utilizzando un linguaggio comune e buone pratiche di facile implementazione.
Gli obiettivi della rubrica sono quelli di informare il lettore sull'evoluzione del mercato Cloud Security e relativi trend tecnologici, buone pratiche, formazione specifica, esperienze sul campo e condividere anteprime dei risultati dei gruppi di lavori di Cloud Security Alliance (più di 20 aree tematiche attive a livello internazionale e 5 a livello nazionale) . I lettori di riferimento non sono soltanto i professionisti dell'information e cyber security, ma vogliamo rivolgerci e coinvolgere anche:

- i **legali**, considerando le novità introdotte dal nuovo regolamento europeo sulla Data Protection e la nuova figura del Data Protection Officer che dovrà occuparsi sempre più di tematiche Cloud (tracciabilità del dato, privacy, safe harbour, digital forensics nel cloud, ...);

Alberto Manfredi è Presidente di CSA Italy dal 2011. Dottore in Scienze dell'Informazione e Dottore Magistrale in Informatica con pieni voti assoluti e lode, lavora da piu` di 20 anni nel settore ICT e Cyber Security. Attualmente lavora in Finmeccanica Spa come Business Development Manager nel Settore Elettronica e Sistemi di Difesa e Sicurezza. Detiene le certificazioni professionali CISA, CRISC, CISSP, GCFA, CCSK, Lead Auditor 27001, Certified CSA STAR Auditor. Cofondatore e Managing Director dell'associazione Club R2GS Europe nata per favorire lo scambio di esperienze e conoscenza nel campo Security Information and Event Management e Security Operation Centres.

CSA Italy è un'associazione no profit italiana nata nel 2011 come capitolo nazionale dell'associazione internazionale CSA (Cloud Security Alliance) a cui aderiscono le maggiori aziende del settore ICT ed Information Security che hanno scelto il Cloud Computing come parte rilevante del loro business. CSA coordina una community di professionisti che contribuiscono attivamente a sviluppare linee guida e buone pratiche per uno sviluppo ed utilizzo in sicurezza del Cloud.

- i **responsabili acquisti/buyer**, perché è necessaria una nuova classificazione dei fornitori Cloud distinta dalla classificazione tradizionale con fornitori software, hardware e telecomunicazioni;
- gli **sviluppatori software**, considerando i nuovi sviluppi di applicazioni su Platform as a Service , metodologie SSDLC e focus su API Security;
- i **manager delle linee di business** che vogliono utilizzare le risorse Cloud come un supporto più efficace ed efficiente alle loro attività;
- **i responsabili strategie**, perché l'introduzione del Cloud in un'azienda richiede un approccio strategico a breve, medio e lungo termine per poterne cogliere tutti i benefici e minimizzare gli impatti;
- **i responsabili organizzazione risorse umane,** perché il nuovo personale, e non solo, è ormai "digital native" ed il mercato propone diversi servizi Cloud per selezionare, formare, collaborare in azienda;

Ci auguriamo che questa rubrica possa essere un "compagno di viaggio" nel vostro percorso verso il Cloud in sicurezza.
Buona lettura! ■

PRESENTAZIONE RUBRICA INFRASTRUTTURE CRITICHE

Luisa Franchina,
Presidente di AIIC

La Rubrica "Infrastrutture critiche" andrà a trattare con periodicità tematiche relative a quelle infrastrutture dalle quali dipende il consueto e lineare svolgimento delle funzioni vitali di uno Stato. La continuità delle funzioni e la sicurezza delle attività in alcuni settori critici sono rilevanti per il loro ruolo strategico ed essenziale a supporto della sicurezza e della vita del Pase.
La Direttiva Europea 2008/114/CE definisce l'infrastruttura critica come "un elemento, un sistema o parte di questo [...] che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo [...] a causa dell'impossibilità di mantenere tali funzioni".
La Direttiva è stata attuata in Italia attraverso il D.Lgs n°61 dell'11 Aprile 2011. Tramite il Decreto Legislativo si acquisiscono inoltre le metodologie e gli strumenti, definiti in ambito europeo, per individuare anche le Infrastrutture Critiche di interesse nazionale.
Fondamentale nella definizione e nella gestione delle Infrastrutture Critiche è l'identificazione dei rischi e degli impatti di una minaccia su di un determinato settore. Le minacce possono essere di tipo naturale – prevedibili o imprevedibili – che nel nostro Paese si individuano in particolare nel rischio idrogeologico, alluvioni, terremoti, attività vulcaniche ed incendi; oppure di natura antropica, sia volontarie come un attacco terroristico, che accidentali, come un errore umano.
L'impatto che tali minacce possono avere sul settore individuato come essenziale, si delinea come uno strumento basilare per permettere di definire la criticità dell'infrastruttura.
L'Unione Europea ha infatti definito come criterio per determinare le Infrastrutture Critiche l'impatto che una crisi potrebbe

Luisa Franchina: Ingegnere elettronico con dottorato e post dottorato di ricerca in ingegneria elettronica (Università di Roma la Sapienza) e master in geopolitica (IASD) del Centro Alti Studi Difesa. Ha conseguito la qualifica militare CBRN presso la Scuola di Rieti. E' stata Direttore Generale della Segreteria per le Infrastrutture Critiche (Presidenza del Consiglio dei Ministri 2010-2013), Direttore Generale del Nucleo Operativo per gli attentati nucleari, biologici, chimici e radiologici (Dipartimento della Protezione Civile 2006-2010) e Direttore Generale dell'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (Ministero delle Comunicazioni 2003-2006). Attualmente ha fondato una azienda che eroga servizi di gestione del rischio, informative e reporting. Docente presso master specialistici presso Sapienza, Tor Vergata, SIOI, Campus Biomedico, Bocconi, Università di Milano, in temi di sicurezza. Ha pubblicato numerosi articoli e libri su temi di sicurezza e protezione infrastrutture critiche.

AIIC - ASSOCIAZIONE ITALIANA ESPERTI IN INFRASTRUTTURE CRITICHE nasce per costruire e sostenere una cultura interdisciplinare per lo sviluppo di strategie, metodologie e tecnologie in grado di assicurare la protezione delle infrastrutture critiche e la loro gestione in situazioni di crisi, di eventi eccezionali o a seguito di atti terroristici.

avere in termini di vittime, di effetti economici (intesi come perdite e deterioramento di prodotti e servizi) e di effetti pubblici, ossia l'impatto sulla fiducia dei cittadini, il turbamento della vita quotidiana e la salute pubblica.
Tra i rischi non naturali acquista sempre più rilevanza, come già riportato, l'utilizzo dello spazio cibernetico. La minaccia si sta infatti evolvendo e ciò permette di individuare nuovi settori critici e di sottolineare la complessità e l'importanza dell'interconnessione tra di essi.
Basti pensare a quante infrastrutture fondamentali sono informatizzate, utilizzano servizi in rete e la tecnologia informatica è centrale o necessaria al loro funzionamento. La lista potrebbe partire dalla stessa infrastruttura di telecomunicazioni e comprendere il settore dell'energia, della salute pubblica, dei trasporti, della finanza e del credito, della pubblica amministrazione, come della difesa e della sicurezza pubblica.
Un esempio ci permette di comprendere con chiarezza il rischio che attraversa lo spazio cibernetico: sono noti e non rari eventi di incidenti, spesso intenzionali e frutto di azioni malevole, che colpiscono i sistemi informatici SCADA, ossia di controllo di supervisione ed acquisizione di dati, demandati al monitoraggio e al controllo di sistemi fisici dei processi industriali. Un attacco cibernetico con potenziali ripercussioni fisiche potrebbe portare all'interruzione ed al deterioramento di processi essenziali, il cui impatto potrebbe risultare considerevole in termini di vittime, di perdita economica e di effetti sulla vita pubblica.
Un valutazione ed una gestione dei rischi per le Infrastrutture Critiche sono quindi necessarie, così come lo è investire risorse nella loro messa in sicurezza e nel miglioramento della loro resilienza e robustezza.
Osservata la potenziale gravità dell'impatto, si può convenire sul fatto che il costo di una mancata sicurezza potrebbe risultare ancor maggiore dell'investimento, soprattutto perché potrebbero essere colpiti elementi vitali di un Paese e delle sue funzioni. Un'analisi dei costi di una scarsa sicurezza permette di osservare sia le potenziali perdite immediate, ma anche quelle indirette, definibili come la mancanza di fiducia nelle istituzioni, la perturbazione dell'ordine sociale e gli effetti reputazionali negativi sulle aziende coinvolte.
Fondamentale è quindi l'osservazione di *best practice* e di standard di sicurezza riconosciuti a livello internazionale ed in particolare definire delle politiche che permettano di gestire ed ottimizzare la sicurezza delle Infrastrutture Critiche in funzione dell'interdipendenza del settore pubblico e privato in tale ambito.
Nel campo della sicurezza delle Infrastrutture Critiche attori pubblici e privati si trovano a cooperare proprio in ragione dell'interconnessione delle infrastrutture stesse, che diventano così realtà più complesse e reciprocamente dipendenti, e che necessitano di coordinamento per affrontare le vulnerabilità che in tale sistema reticolare potrebbero portare ad un pericoloso effetto domino.
Tale interconnessione è ancor più rilevante ed evidente nello spazio cibernetico, dove – come sottolineato anche dal DPCM del 24 Gennaio 2013 – la gestione della sicurezza è compito tanto delle realtà pubbliche quanto delle società private.
In questo scenario acquisisce un valore particolare l'*information sharing* tra gli operatori delle Infrastrutture Critiche, che permette un'amministrazione più efficace delle interconnessioni, condividendo informazioni relative ai rischi, alle minacce, alle soluzioni adottate ed alle pratiche di sicurezza che permettano di rispondere con reattività ed organicità ad una situazione di crisi condivisa.
Gli articoli che troveranno spazio all'interno di questa rubrica si occuperanno di analizzare e di approfondire argomenti e questioni relative alle Infrastrutture Critiche ed alla loro protezione.
Si parlerà di aspetti normativi, di standard e *best practice* per la sicurezza, dei rischi e del loro *management*. Un ruolo di primo piano lo occuperanno gli approfondimenti sulla cyber security, sull'esame dell'evoluzione delle minacce e sulla collaborazione tra settore privato e pubblico. Non mancheranno gli aggiornamenti relativi alle *news* ed agli eventi del settore. ■

LA MINACCIA TERRORISTICA ALLA SICUREZZA E ALLE INFRASTRUTTURE CRITICHE NAZIONALI

Un modello di analisi dei rischi

Luisa Franchina,
Presidente di AIIC

Ludovica Coletta,
Dottoressa in Relazioni Internazionali presso l'Università Luiss Guido Carli

Il fenomeno del terrorismo di matrice islamica è un pericolo attuale e concreto che persisterà anche nel medio e lungo periodo negli elenchi delle minacce prioritarie delle agende nazionali. Se a ciò si aggiunge il crescente attivismo di tipo molecolare, si comprende come la complessità dello scenario sia, oggi giorno, estrema. Per di più, se da un lato il lavoro dei Servizi di informazione è stato facilitato dai progressi nel campo della tecnologia che hanno giovato alle tecniche d'intelligence, dall'altro ci si trova a fronteggiare una minaccia sempre meno "visibile" e prevedibile.

L'analisi svolta intende esaminare la minaccia terroristica di matrice islamica ponendola in relazione con le infrastrutture critiche nazionali, quali target di possibili attentati e proponendo un'analisi dei rischi che tenga conto delle tipologie d'attacco, fermo restando l'elevato tasso di imprevedibilità della minaccia stessa, derivante dalla crescente interconnessione fra i gruppi fondamentalisti (nella loro interezza, in parte o a livello di singole affiliazioni), nonché dall'azione emulativa di lupi solitari. Molti paesi europei ed extraeuropei si sono già da tempo dotati di piani di sicurezza in materia di infrastrutture critiche che permettono di identificare quelle d'importanza strategica e di formulare sistemi di protezione. L'individuazione – all'interno di un documento *ad hoc* che rispecchi le direttive europee e definisca una strategia di difesa unitaria, organica e di sistema – delle infrastrutture di rilevanza critica e strategica per il sistema paese è di fondamentale importanza in un momento, come quello attuale, in cui tali infrastrutture sono esposte a molteplici minacce, non convenzionali e multiformi, tra cui quella di matrice terroristica. Una strategia che permetta ai vari soggetti incaricati di "fare sistema" consentirebbe, dunque, di assicurare un maggiore e migliore coordinamento in fase di risposta ad attacchi di qualsiasi genere contro tali infrastrutture.

A tal fine, l'intento dell'elaborato è quello di fornire un diverso spunto di riflessione su un tema caldo come quello del terrorismo di matrice islamica, ponendolo in connessione con le metodologie di analisi strategica e protezione del sistema paese. Nello specifico, a partire dall'individuazione delle infrastrutture critiche a livello nazionale e sulla base del modello di Enterprise Risk Management, è stata proposta una doppia analisi dei rischi che tiene conto delle varie tipologie di attacco (terrestri, aeree e cibernetiche) e dei possibili obiettivi in qualità, appunto, di settori critici. In seguito, a ciascun rischio identificato è stato attribuito un indice numerico, sulla base di una scala di valori crescenti per probabilità e impatto, nonché di una valutazione del grado di pericolosità della minaccia terroristica nel nostro paese.

Questo tipo di analisi consente di effet-

tuare un discrimine e un focus sugli asset che presentano un maggiore indice di rischio e sui quali va posta una speciale attenzione in termini di prevenzione e protezione: distinzione che potrebbe risultare utile ad un eventuale decisore, soprattutto alla luce della necessaria allocazione delle risorse (umane ed economiche), spesso limitate, sul territorio. Di seguito è illustrato con maggior dettaglio un estratto dell'analisi svolta[1] che ha come focus gli attacchi cibernetici ed i grandi eventi.

Sulla base della definizione declinata nella Direttiva 2008/114/CE, sono state individuate le infrastrutture critiche di rilevanza strategica in relazione alla minaccia in esame.

Partendo dal modello dell'Enterprise Risk Management (ERM), una prima analisi è stata svolta prendendo in considerazione le diverse tipologie di attacco terroristico, mentre una seconda a partire dai settori critici elencati in precedenza. Le metriche utilizzate per le matrici di probabilità – impatto provengono da una matrice di base composta da cinque livelli di probabilità e di impatto (dal "very low" al "very high"), i cui colori si riferiscono a tre diverse tipologie di risposta al rischio, dal trascurabile al non accettabile.

1 Estratto dall'elaborato "Minacce alla sicurezza e alle infrastrutture critiche nazionali da parte dei movimenti del fondamentalismo islamico. Il ruolo dei Servizi di Informazione" redatto a conclusione del Master in Sicurezza delle Informazioni ed Informazione Strategica dell'Università degli Studi di Roma "La Sapienza".

INFRASTRUTTURE CRITICHE
AGGREGATION SITES, MONUMENTS and ICONS
SPECIAL EVENTS
SOFT TARGET
GOVERNMENT and INSTITUTIONAL SITES
TRANSPORT
ENERGY
ICT and MEDIA

				I - Impatto				
				Very Low	Low	Medium	High	very High
				X ≤ 10%	10% < X ≤ 25%	25% < X ≤ 50%	50% < X ≤ 75%	X > 75%
			Valore I	0,5	1	2	4	8
			Valore P					
P - Probabilità	Very High	X > 75%	9	5	9	18	36	72
	High	50% < X ≤ 75%	7	4	7	14	28	56
	Medium	25% < X ≤ 50%	5	3	5	10	20	40
	Low	10% < X ≤ 25%	3	2	3	6	12	24
	Very Low	X ≤ 10%	1	1	1	2	4	8

ANALISI DEI RISCHI SULLA BASE DELLE TIPOLOGIE D'ATTACCO

Le tipologie di attacco terroristico che potrebbero essere adottate per compiere attentati sul territorio nazionale sono state individuate sulla base di un'analisi dei precedenti attentati, nonché dell'effettiva disponibilità degli strumenti di offesa in capo agli attaccanti e sono state aggregate in tre classi: attacchi da terra, aerei e cyber. Tra gli attacchi terrestri si inquadrano gli attentati suicidi, le autobomba, gli ordigni esplosivi (anche CBRN), gli assalti armati e gli attacchi CBRN; tra quelli aerei i dirottamenti e i missili e, infine, tra gli attacchi cyber si includono i defacement, i malware, i furti di dati e credenziali e gli attacchi DDoS. Ad ogni tipologia di attacco è stato successivamente associato un elenco di possibili obiettivi in termini di infrastrutture critiche. Per calcolare il relativo indice di rischio, inteso come il prodotto fra probabilità e impatto, a partire dalla matrice di base ne sono state individuate quattro, rappresentative degli impatti in termini di vittime, danni economici, risonanza mediatica e conseguenze politico-sociali. Sul versante degli attacchi cyber, i risultati dell'analisi puntano una particolare attenzione sullo strumento dei malware, in grado i produrre impatti anche in termini di vittime (valore che per le altre tipologie di attacco risulta essere pressoché nullo). Tra i settori critici che potrebbero essere maggiormente colpiti dalle conseguenze di eventuali attacchi cibernetici si registrano quelli governativi, dei trasporti, ICT e media, energetici, finanziari, della difesa e dell'industria CBRN.

CYBER									
ID attacco	Tipologia di attacco	ID Obiettivo	Obiettivi	P	I_V	I_E	I_M	I_PS	Max Score
C_1	Defacement	C_1.1	Special events	5	0	0,5	1	1	5
		C_1.2	Soft Target	7	0	0,5	2	1	14
		C_1.3	Government and institutional sites	7	0	0,5	4	1	28
		C_1.4	ICT and media	7	0	0,5	2	1	14
		C_1.5	Energy	5	0	0,5	2	1	10
		C_1.6	Finance	5	0	0,5	4	1	20
		C_1.7	Defence	7	0	0,5	4	1	28
C_2	Malware	C_2.1	Soft Target	5	0,5	0,5	1	1	5
		C_2.2	Transport (rail)	3	2	8	4	2	24
		C_2.3	Transport (air)	3	2	8	4	2	24
		C_2.4	Government and institutional sites	5	0,5	0,5	2	2	10
		C_2.5	Energy	3	1	8	4	2	24
		C_2.6	ICT and media	3	0,5	1	2	1	6
		C_2.7	Finance	3	0,5	8	4	2	24
		C_2.8	Defence	3	0,5	0,5	1	1	3
C_3	Furto credenziali e dati	C_3.1	Government and institutional sites	3	0	4	4	2	12
		C_3.2	ICT and media	3	0	4	1	1	12
		C_3.3	Energy	3	0	8	2	1	24
		C_3.4	Finance	3	0	8	2	1	24
		C_3.5	Defence	3	0	2	1	1	6
C_4	DDoS	C_4.1	Special events	1	0	1	4	2	4
		C_4.2	Soft Target	1	0	1	1	1	1
		C_4.3	Government and institutional sites	3	0	1	4	2	12
		C_4.4	ICT and media	3	0	1	2	1	6
		C_4.5	Energy	3	0	1	2	1	6
		C_4.6	Finance	3	0	1	4	1	12
		C_4.7	Defence	1	0	1	2	1	2

ANALISI DEI RISCHI SULLA BASE DELLE INFRASTRUTTURE CRITICHE

La seconda analisi del rischio è stata condotta a partire dalle infrastrutture critiche individuate in precedenza, utilizzando la medesima tassonomia adottata per la prima analisi. Tra i vari settori che sono stati presi in considerazione, quello dei grandi eventi continua ad essere vulnerabile agli attacchi terroristici a causa della relativa facilità con cui si potrebbe realizzare un attentato e degli altissimi impatti (in primis in termini di vittime) che ne conseguirebbero. Con il termine grandi eventi si intendono quelle manifestazioni pubbliche che assumono particolare rilievo per "*rilevanza o popolarità a livello storico e politico; ampia risonanza nei media e/o partecipazione dei media a livello internazionale; partecipazione dei cittadini di diversi paesi e/o di eventuali gruppi destinatari; partecipazione di VIP e/o personalità; alto numero di persone*". In tal senso, si intendono grandi eventi l'EXPO di Milano, il Giubileo, i vertici internazionali, nonché importanti eventi sportivi di risonanza mondiale (finali di calcio, olimpiadi, tornei internazionali).

La salvaguardia della sicurezza nei grandi eventi è essenziale per diversi motivi, dalla protezione e l'incolumità dei cittadini, alla tutela degli investimenti economici, fino alla protezione dell'immagine del paese a livello interno (come tenuta del sistema di governo) e internazionale (in termini di credibilità). A differenza dei luoghi di aggregazione, non sempre è possibile individuare con precisione l'area perimetrale di un grande

SPECIAL EVENTS : EXPO, GIUBILEO, MARATONA, EVENTI SPORTIVI INTERNAZIONALI, VERTICI INTERNAZIONALI					
ID rischio	**Descrizione del rischio**	**KRI**	**P**	**I**	**Score**
SE_1	Assenza di sistemi di controllo accessi basati sul riconoscimento facciale (sulla base di un database pre-caricato di possibili	n° discpositivi di riconoscimento facciale / n° dispositivi	3	8	24
SE_2	Sistemi di controllo accessi insufficienti per addetti ai lavori e utenti (tornelli, macchine vidimatrici, ecc...)	n° personale addetto alla sicurezza effettivamente presente / n° personale ottimale ; n° metal detector o body scanner effettivi / n° ottimale; implementare politiche di controllo accessi (badge elettronici, videosorveglianza, sorveglianza armata, riconoscimento facciale ecc)	5	8	40
SE_3	Personale di sicurezza impreparato/insufficiente	n° personale effettivo / n° personale; implementazione politiche e tecniche d'intervento (procedure di accreditamento, controllo della folla, capacità di identificare terroristi, sventare attentati, ecc); monitoraggio grado di formazione degli steward	3	4	12
SE_4	Accessi di servizio incontrollati (seppure per periodi parziali)	monitoraggio accessi di servizio (registri, videosorvegianza, vigilanza, ecc)	5	8	40
SE_5	Sistemi informatici e di comunicazione insufficienti e/o	monitoraggio livello di efficienza e sicurezza dei sistemi; aggiornamento	5	2	10
SE_6	Procedure di emergenza non definite e/o scarse e/o non aggiornate/testate sufficientemente	monitoraggio adeguatezza agli standard; monitoraggio n° test/aggiornamenti annui; monitoraggio ore dedicate alle procedure di emergenza	3	8	24
SE_7	Scarsa condivisione database con profili dei terroristi ai fini del riconoscimento	monitoraggio livello di diffusione dei database; monitoraggio effettiva condivisione e ricezione dei database	3	8	24
SE_8	Scarsa adozione di misure e tecnologie d'individuazione di esplosivo/materiale chimico o	monitoraggio livello di investimenti e sviluppo in tecnologie d'individuazione di esplosivo/materiale chimico o batteriologico	3	8	24
SE_9	Scarsa integrazione fra i sistemi di sicurezza	monitoraggio livello di integrazione	5	4	20

evento. Nel caso del Giubileo, ad esempio, il perimetro non è circoscritto solamente al Vaticano, ma comprende più aree a rischio come il sistema dei trasporti, i monumenti o i musei.
Di conseguenza, uno dei maggiori rischi evidenziati nell'analisi, connesso a questo tipo di infrastruttura, potrebbe derivare da un'insufficienza dei sistemi di controllo accessi in termini di incapacità di definizione di un'area perimetrale da controllare, di scarsità di personale (con conseguenti accessi secondari incontrollati) o di insufficiente preparazione dello stesso. Il personale di sicurezza dovrebbe essere sempre addestrato e pronto a rispondere a qualsiasi emergenza: in tal senso andrebbero periodicamente effettuate prove di emergenza e simulazioni per rendere gli addetti pronti a gestire la folla, sventare attentati e identificare potenziali attaccanti prima che colpiscano.
Ulteriore elemento essenziale dovrebbe essere il costante coordinamento informativo fra le forze di polizia e i servizi di informazione in merito alla diffusione di allarmi e database contenenti le informazioni relative a persone sospette e terroristi.
Tali database dovrebbero essere a disposizione del personale operativo in strada e dovrebbero essere pre-caricati sui sistemi di videosorveglianza a riconoscimento facciale. In tal senso, al lavoro di addestramento e formazione del personale si dovrebbe accostare un adeguato sistema di supporto tecnologico in grado non solo di identificare i terroristi (telecamere) o armi (metal detector), ma anche di individuare materiale esplosivo o chimico/batteriologico.

CONCLUSIONI

Il cyber crime e il terrorismo molecolare costituiscono senza dubbio le minacce prioritarie del presente e del prossimo futuro. Nel fronteggiare tali pericoli, un'analisi come quella proposta può essere di aiuto se affiancata ad altre metodologie di intelligence. In tal senso, la centralità dell'OSINT rimane infatti cruciale: avvalersi di tecnologie di ricerca e di analisi semantica in grado di filtrare ed estrapolare le informazioni necessarie dalle innumerevoli fonti aperte permette di facilitare il lavoro degli analisti e di velocizzare le ricerche.
Allo stesso tempo, all'organico di analisti e di tecnologie informatiche va abbinato il ruolo della HUMINT, la quale, unita a un buon livello di coordinamento informativo a livello nazionale ed internazionale tra le Agenzie di informazione, costituisce un perno di importanza strategica per lo sviluppo delle capacità possedute dai professionisti del mestiere, nonché per il mantenimento di contatti diretti con le zone di interesse che possano fornire informazioni aggiuntive all'analisi o possano verificare informazioni già ottenute tramite le fonti tecnologiche. ■

www.eset.it

ENJOY SAFER TECHNOLOGY™ eset

PROTEZIONE TOTALE PER LA TUA AZIENDA

- ENDPOINT ANTIVIRUS
- ENDPOINT SECURITY
- MOBILE SECURITY
- FILE SECURITY
- MAIL SECURITY
- BACKUP E RIPRISTINO
- AUTENTICAZIONE A 2 FATTORI
- GATEWAY SECURITY
- SHAREPOINT SECURITY
- AMMINISTRAZIONE CENTRALIZZATA
- CRITTOGRAFIA DEI DATI

UNA TECNOLOGIA FRA LE MIGLIORI AL MONDO CHE NON RALLENTA I TUOI SISTEMI E NON INTRALCIA IL TUO LAVORO.

ESET Mobile Security
Proteggi **gratuitamente** il tuo cellulare e il tuo tablet Android.

MIGLIORE DEL TEST
Test 06.2015
altroconsumo.it/label
ADMT15001
ALTROCONSUMO

ESET Smart Security 8 è Migliore del Test Altroconsumo

FUTURE TIME
tecnologie antivirus

DIVENTA RIVENDITORE
partners.eset.it

PRESENTAZIONE RUBRICA FATTORE UMANO E AMBIENTE DIGITALE

Isabella Corradini,
Presidente Centro Ricerche Themis Crime

In questi ultimi anni si è rafforzata la convinzione che la gestione della sicurezza sia fortemente correlata al fattore umano. Che si tratti di sicurezza in ambito informatico, di sicurezza fisica o di sicurezza sul lavoro, la questione non cambia: l'adozione da parte delle persone di comportamenti prudenti può fare realmente la differenza nelle strategie di prevenzione.

Le persone si muovono negli ambienti digitali, una ricchezza alla quale non si può e non si deve rinunciare ma che richiede cautela: l'esposizione delle identità digitali è tale che i rischi per la sicurezza sono un problema da affrontare, tra furti di identità, frodi, violazioni dei dati, cyberspionaggio, solo per fare qualche esempio. Gli schemi di attacco si fanno sempre più sofisticati, ma anche tecniche note agli esperti da anni sono sempre più diffuse: è il caso degli attacchi di ingegneria sociale, tecniche conosciute da sempre e particolarmente potenti poichè, sfruttando principi psicologici, agiscono sulla percezione dell'utente, influenzandone il comportamento.

L'evoluzione tecnologica non si arresta e con l'Internet delle cose (IoT) si prevedono nei prossimi anni a venire miliardi di dispositivi connessi. Questi cambiamenti richiedono di considerare con attenzione gli aspetti di sicurezza, dal momento che si moltiplicheranno dati e informazioni tra i dispositivi collegati in Rete; così come è importante considerare la necessità per le persone di adattarsi ad uno stile di vita in cui tutto sarà interconnesso.

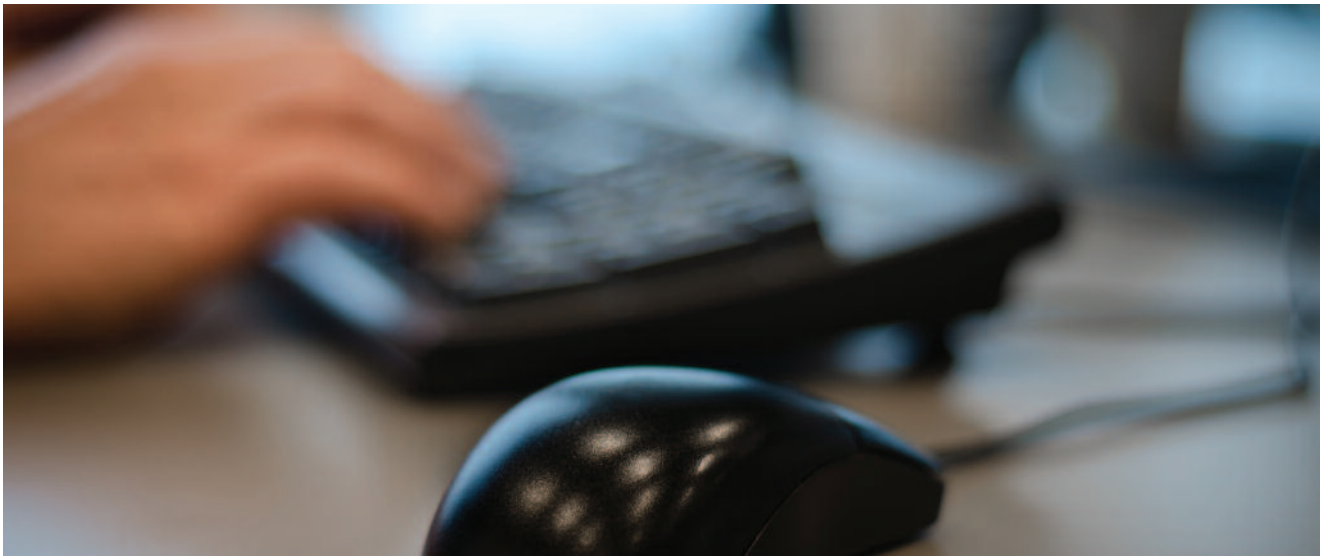
Da sempre fautrice dell'importanza del fattore umano nella sicurezza, con questa rubrica Isabella Corradini inaugura uno spazio dedicato alla lettura dei fenomeni cyber con un approccio umanistico e sociale, sottolineando l'importanza della relazione tra uomo e tecnologie. Considerando che le tecnologie, e in particolare le tecnologie dell'informazione, incidono fortemente sulla dimensione individuale e globale, è evidente che nell'affrontare i temi della sicurezza informatica non si può prescindere dalla conoscenza dei meccanismi umani e sociali.

Ambiente digitale, comportamenti umani, organizzazioni, cultura, ricerca, formazione, comunicazione, reputazione: queste alcune parole delle parole chiave che caratterizzano i temi della rubrica.■

Isabella Corradini, Psicologa sociale e del lavoro, criminologa, è esperta sui temi della sicurezza (safety, security e cybersecurity) con approccio psicosociale e in comunicazione aziendale. E' Presidente e Direttore Scientifico del Centro Ricerche Themis e responsabile di Reputation Agency. Ha di recente fondato con Enrico Nardelli il Link&Think Research Lab per lo sviluppo di attività di ricerca interdisciplinare. Presso l'Università dell'Aquila, Dipartimento di Medicina Clinica, Sanità pubblica, Scienze della Vita e dell'Ambiente, insegna psicologia sociale e psicologia del comportamento criminale. E' docente in corsi di perfezionamento e master presso diverse Università italiane in materia di psicologia, sicurezza, comunicazione e reputazione. E' membro scientifico di diversi comitati editoriali e tecnici, e autrice di numerose pubblicazioni. Sul tema della reputazione è curatore di una collana per la Franco Angeli Editore e responsabile scientifico della rivista Reputation Today.

SICUREZZA DEI DATI, TRA PASSWORD E COMPORTAMENTI

Tra i consigli che gli specialisti di sicurezza ci forniscono per tutelare i nostri account c'è l'attenzione che occorre prestare alla scelta della password, la quale deve essere complicata e soprattutto "robusta", per evitare che sia facilmente scoperta. Così facendo, però, scegliere una password può diventare faticoso, visto il numero elevato di account che ormai tutti possediamo, anche se è comunque un'operazione necessaria per garantire al meglio la tutela dei propri dati personali.
Gli utenti devono essere consapevoli dell'importanza del loro comportamento nel prevenire furti di credenziali e violazioni da parte di cybercriminali.
Una politica di prevenzione deve essere messa in atto anche dai siti ai quali gli utenti si registrano, ad esempio inducendoli ad adottare password efficaci. Si pensi a quanto questo possa essere importante – in particolare – per i siti e-commerce per il quali la sicurezza dei clienti è ciò che garantisce il loro business.
Violazioni di dati e abusi si riflettono inevitabilmente sulla reputazione e sul business; per questo essi devono adottare tutte le misure e le precauzioni necessarie per proteggere i dati dei propri clienti.
Il fenomeno della violazione dei dati è ormai un problema che non può essere assolutamente sottovalutato.
Nessuno, infatti, può ritenersi invulnerabile. Mettere in campo tutte le cautele del caso, sia di tipo tecnico-organizzativo che comportamentale, diventa pertanto un passaggio necessario se si vogliono ridurre il più possibile i rischi di subire violazioni.
Nella terza edizione del barometro di Dashlane, società specializzata nella gestione di password e identità on line, gli



esperti hanno analizzato il modo con cui i siti di e-commerce (che vendono in Francia) gestiscono la sicurezza delle password.
Secondo l'indagine, il 52% dei 25 siti analizzati non impone ai loro visitatori l'utilizzo di password complesse, mettendo così a rischio la sicurezza dei dati personali dei loro clienti.
Il 36% accetta password facili da ricordare - ma anche da hackerare - come il classico "123456".
La valutazione Dashlane produce un punteggio compreso tra -100 e +100 calcolato sulla base di una serie di criteri che attribuiscono valori negativi a misure particolarmente carenti dal punto di vista della sicurezza e punteggi positivi per misure particolarmente buone. Tra i criteri negativi, ad esempio, vi è l'accettazione di password banali create dall'utente; tra quelli positivi l'obbligo per l'utente di usare numeri ed altri caratteri non alfabetici per la creazione della password.
Analizzando il barometro Dashlane si rimane sorpresi nel trovare in questa classifica siti e-commerce importanti con punteggi negativi (tabella 1).
Nella tabella 2 vengono invece riportati i siti e-commerce con un punteggio positivo. Tra questi al primo posto si colloca Apple con uno score di 100.
Una comparazione tra il barometro del 2015 e quello del 2014 evidenzia alcuni elementi interessanti, come la crescita di consapevolezza di alcuni siti nel rafforzare la protezione dei dati dei loro clienti. Ad esempio, si legge nel nuovo barometro che Alloresto, Vente Privée, Cdiscount e Show Room Privé impongono ora ai loro utenti la creazione di password più robuste rispetto al passato (nella comparazione tra i due anni va tenuto conto che il numero dei siti analizzati è cresciuto).
Certo, il principio fondamentale è che, a prescindere dalle sollecitazioni rivolte all'utente da parte dei siti, egli deve comunque essere consapevole dei rischi ai

Siti con punteggio negativo	Score
Aramis Auto	-65
Amazon France	-60
Castorama	-60
Ldlc	-50
Oscaro	-45
La Redoute	-40
Rue du Commerce	-40
Zalando	-35
Sarenza	-30
Leroy Merlin	-26

Tabella 1 – I 10 siti con punteggio più negativo

quali può andare incontro se non rispetta semplici regole di sicurezza, come la scelta di password efficaci.
Ma di fronte alla naturale tendenza dell'essere umano a risparmiare energie (anche cognitive) e a pensare di poter controllare tutto ciò che lo circonda, non di rado si commette l'errore di sottovalutare l'importanza di alcuni comportamenti di tutela. In aggiunta, come superare il problema di dover ricordare tutte le password create a fronte di un numero sempre più elevato di account?
Di sicuro interesse è la proposta di due ricercatori della University of Southern California, Ghazvininejad e Knight che, in convegno di linguistica computazionale tenuto nel giugno del 2015 hanno proposto una soluzione insolita ma efficace: è possibile creare delle password robuste ricorrendo a brevi poesie. Per essere ricordate devono essere in rima e per resistere agli attacchi non devono essere componimenti noti.
I due studiosi hanno realizzato un generatore casuale di password (da usare solo a scopo dimostrativo) ed i loro esperimenti evidenziano che tali password si ricordano più facilmente e sono meno attaccabili.
Di certo, in un ambiente sempre più digitale, strutture e persone devono interagire per garantire al meglio la sicurezza. Gli strumenti ci sono, vanno applicati con rigore e costanza. ■

RIFERIMENTI

http://www.itrpress.com/cp/2016/2016-01-06_dashlane.pdf

http://blog.dashlane.com/wp-content/uploads/2014/03/UK-Methodology.pdf

http://www.bancaforte.it/notizie/2016/01-2/una-poesia-come-password

http://www-scf.usc.edu/~mghazvin/papers/marjan15.pdf

http://www.isi.edu/natural-language/people/poem/poem.php

Siti con punteggio positivo	Score
Apple	100
Auchan	95
Alloresto	75
Cdiscount	75
Carrefour	50
Price Minister	40
Ebay	30
Vente privée	30
Darty	6
Fnac	5

Tabella 2 – I 10 siti con punteggio più positivo

PRESENTAZIONE RUBRICA CYBER SPAZIO E SICUREZZA NAZIONALE

Stefano Mele
of Counsel di Carnelutti Studio Legale Associato e Socio Fondatore di Moire Consulting Group

L'elevata pervasività delle tecnologie e della rete Internet in ogni strato dell'odierno tessuto sociale ha completamente trasformato – in un lasso di tempo peraltro esiguo – ogni aspetto della nostra società, dell'erogazione e gestione dei servizi, dell'accesso alle informazioni, della loro qualità e quantità, nonché dell'interazione tra questi elementi e il cittadino.
Come se ciò non bastasse a sottolineare il loro ruolo cruciale nella cosiddetta 'società dell'informazione', le tecnologie e la rete Internet sono ormai alla base anche dei sistemi complessi che assicurano la corretta esecuzione dei settori strategici e sensibili di uno Stato, come quelli dell'energia, delle comunicazioni, dei trasporti, della finanza e così via. Esse rappresentano, quindi, uno dei principali cardini intorno a cui ruota il benessere economico e sociale di ogni Stato, nonché il piano di appoggio e il motore della sua crescita.
Peraltro, l'analisi dello scenario corrente e dei principali documenti strategici nazionali in ambito di *cyber-security* delinea contorni particolarmente evidenti delle direttrici di minaccia, causate principalmente dallo scarso livello di percezione e consapevolezza di queste problematiche, dal vuoto normativo e di regolamentazione sovrannazionale del settore, dal debole livello di collaborazione interna e internazionale, nonché dalla scarsa capacità di raggiungere un adeguato *standard* di sicurezza informatica e di resilienza dei sistemi critici nazionali.
Garantire un approccio strategico alla sicurezza di questo settore, pianificarne la crescita, valutare i rischi a breve, medio e lungo termine, nonché svolgere attività previsionali sulla sua evoluzione, rappresentano, quindi, un compito ormai imprescindibile, da porre come prioritario nell'agenda politica di ogni buon governo, soprattutto oggi che la protezione del cosiddetto 'spazio cibernetico' rappresenta per tutti una sfida ad elevato grado di priorità.
Questa rubrica si pone come scopo quello di sensibilizzare il lettore su questi argomenti, analizzando i principali avvenimenti a livello internazionale, al fine di trarre i *trend* della 'minaccia cibernetica' e le "lezioni apprese" utili alla salvaguardia della nostra sicurezza nazionale. ■

Stefano Mele è avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza delle Informazioni e Intelligence. Lavora a Milano come 'of Counsel' di Carnelutti Studio Legale Associato. E' socio fondatore e Partner del Moire Consulting Group ed è Presidente del "Gruppo di lavoro sulla cyber-security" della Camera di Commercio Americana in Italia.
È Direttore di Ricerca su Cyber-security & Cyber-Intelligence del Ce.Mi.S.S. ed è Coordinatore dell'Osservatorio InfoWarfare e Tecnologie emergenti dell'Istituto Italiano di Studi Strategici 'Niccolò Machiavelli'. È inoltre docente presso istituti di formazione e di ricerca del Ministero della Difesa italiano e della NATO, nonché autore di numerose pubblicazioni scientifiche e articoli sui temi della cyber-security, cyber-intelligence, cyber-terrorism e cyber-warfare. Nel 2014, la NATO lo ha inserito nella lista dei suoi Key Opinion Leaders for Cyberspace Security e la rivista Forbes lo ha inserito tra i 20 migliori Cyber Policy Experts al mondo da seguire in Rete.

CYBER STRATEGY & POLICY BRIEF (GENNAIO 2016)

I mesi a cavallo tra la fine del 2015 e l'inizio del 2016 sono stati caratterizzati da numerosi e importanti avvenimenti in materia di cyber-security, che non possono assolutamente essere ignorati dagli analisti. Dalla pubblicazione di alcuni fondamentali documenti strategici, fino alla conduzione di attacchi informatici nei confronti di infrastrutture critiche nazionali, il settore continua ad essere caratterizzato da una fortissima espansione e da un elevato numero di attacchi tesi a minare la sicurezza nazionale ed economica dei principali attori presenti sullo scacchiere internazionale. L'approccio strategico degli Stati, peraltro, sta velocemente mutando da una mera difesa attiva (Active Cyber-Defence) ad un vero e proprio sviluppo di capacità offensive per il cyber-spazio. Tutto ciò senza una chiara conduzione strategica a livello sovrannazionale e senza, soprattutto, un substrato internazionale di norme per l'utilizzo delle capacità offensive che sia globalmente condiviso ed accettato.
Di seguito, quindi, vengono brevemente analizzate le principali notizie e i più importanti avvenimenti in materia di cyber-security che hanno caratterizzato questi ultimi mesi.

CINA

Lo scorso 31 dicembre, la *Central Military Commission* cinese ha pubblicamente annunciato di aver completato una sostanziale riforma organizzativa della *People's Liberation Army*, ovvero le Forze Armate cinesi, dando alla luce tre nuovi organismi: l'*Army Leading Organ*, la *Rocket Force* e la *Strategic Support Force*.
Tra le tre, la *Strategic Support Force* appare essere la più interessante sotto il punto di vista della *cyber-security*. Infatti, secondo alcune fonti, sarebbe a sua volta costituita da tre ramificazioni: la prima, responsabile delle operazioni di intelligence e militari nel e attraverso il cyber-spazio (sia difensive, che offensive); la seconda, deputata alle operazioni militari condotte nello spazio, in cui rientrerebbero anche le attività di sorveglianza e quelle inerenti ai satelliti; la terza, infine, con compiti di *electronic warfare* (EW), sia dal punto di vista offensivo, che difensivo e di *intelligence* (ELINT). Ad un'attenta analisi, quindi, la *Strategic Support Force* racchiuderà presto in sé le specialità e le competenze del *Terzo* e del *Quarto Dipartimento* della *People's Liberation Army*, ponendo sotto un'unica linea di comando due dei tre 'domini critici' delineati dal governo cinese all'interno delle sue strategie, ovvero il cyber-spazio e lo spazio (il terzo 'domino critico', invece, è il nucleare).
Questa scelta organizzativa sicuramente non stupisce, né tantomeno deve sorprendere. L'approccio strategico cinese,

infatti, ha da sempre privilegiato da un lato la fusione tra il *cyber-warfare* e l'*electronic warfare*, creando un approccio di "*Intergrated Network and Electronic Warfare*", mentre dall'altro ha favorito l'evoluzione del concetto di *information warfare* verso quello di "*Information Confrontation*". Racchiudere tutti gli elementi dell'*information warfare* – sia militari, che di intelligence; sia difensivi, che offensivi; sia elettronici, che informatici – all'interno di un unico 'contenitore' e sotto una singola ed univoca linea di comando più vicina, rispetto al passato, all'influenza della *Central Military Commission* cinese era il passo successivo e quello più ovvio dal punto di vista strategico.

REGNO UNITO

Da tempo il Regno Unito si è posto come il principale attore europeo in materia di *cyber-security*, sia sotto il punto di vista strettamente legato allo sviluppo economico del settore sul proprio territorio, attraverso, ad esempio, fortissime agevolazioni per le imprese che fanno delle tecnologie e dell'innovazione tecnologica il loro *core business*, che sotto il punto di vista della sicurezza nazionale dalle 'minacce cibernetiche'. In quest'ottica, il 23 novembre 2015, il Regno Unito ha pubblicato il suo nuovo "*Strategic Defense and Security Review*", uno dei documenti più rilevanti per comprendere la postura strategica del governo inglese in ambito di difesa e sicurezza nazionale per i prossimi cinque anni. All'interno di questo documento anche la *cyber-security* viene presa in considerazione e, anzi, proprio la *cyber-defence* – insieme all'intelligence e al contro-terrorismo – rappresenta uno dei settori con la maggior crescita di risorse economiche dedicate. Il Regno Unito, del resto, non è nuovo a quest'approccio, basti pensare che dal 2011 ha già investito 860 milioni di *pound* in questo settore e la previsione è di investirne 1 miliardo e 900 milioni nei prossimi cinque anni. La 'minaccia cibernetica', infatti, viene considerata nel nuovo documento strategico come una delle quattro principali priorità per il governo inglese da qui al 2020.

Pertanto, lo "*Strategic Defense and Security Review*" fissa le principali priorità strategiche in ambito di *cyber-security* previste dal Regno Unito. Esse sono:

- sviluppare una serie di misure per difendere attivamente il Regno Unito dagli attacchi informatici (*Active Cyber-Defence*);
- investire nella creazione di capacità atte a rilevare e analizzare le 'minacce ciber-

netiche', prevenire gli attacchi informatici e rintracciarne i responsabili;
- migliorare la capacità nazionale di rispondere rapidamente ed efficacemente ai cyber-attacchi. Per raggiungere questo obiettivo, il governo britannico creerà un nuovo "*National Cyber Centre*". Il Centro opererà sotto la guida del GCHQ e avrà l'incarico di gestire la risposta agli incidenti informatici sul piano operativo, garantendo così la protezione del Regno Unito dagli attacchi e riducendo al minimo possibile il loro impatto;
- costruire una nuova e più sicura rete intergovernativa per migliorare lo scambio di informazioni e la cooperazione sulle tematiche di *cyber-security*;
- aiutare le aziende e i cittadini a fare di più per proteggere i propri dati dalle 'minacce cibernetiche', fornendo informazioni specialistiche. Ciò avverrà semplificando e rendendo più agevole possibile l'accesso del settore privato alle consulenze in materia di *cyber-security* del governo. In quest'ottica, il nuovo "*National Cyber Centre*" sarà il punto unico di contatto per le aziende in cerca di questo genere di informazioni;
- creare una nuova unità di intelligence specificamente dedicata alla lotta contro l'uso criminale del '*Dark Web*';
- fare in modo che le Forze Armate inglesi raggiungano un eccellente livello di *cyber-defence* e che, in caso di un significativo incidente informatico nel Regno Unito, siano pronte a fornire assistenza. Il governo, inoltre, prevede che le Forze Armate inglesi conseguano capacità militari offensive avanzate attraverso il cyber-spazio, così come previsto dal "*National Offensive Cyber Programme*" gestito in *partnership* dal Ministero della Difesa inglese e dal GCHQ;
- continuare a collaborare con la NATO e con gli altri alleati per proteggere le loro reti informatiche attraverso le informazioni di intelligence e le tecniche di protezione sviluppate dal Regno Unito.

Ciò che emerge e deve urgentemente emergere – anche in un'ottica di sicurezza nazionale dell'Italia – dalla lettura dello "*Strategic Defense and Security Review*" è che il governo del Regno Unito ha sottolineato con forza l'esigenza per le proprie Forze Armate di migliorare le capacità di *cyber-defence*, ma, soprattutto, di sviluppare eccellenti e avanzate capacità militari offensive per il cyber-spazio a sostegno degli interessi nazionali e di quelli della coalizione. Ciò rende il governo inglese uno dei pochissimi Stati ad aver ufficialmente formalizzato in una *policy* l'uso offensivo degli attacchi informatici. Urge, pertanto, che il medesimo dibattito sia portato quanto prima ai più alti livelli anche in Italia, soprattutto oggi che gli attacchi informatici alle infrastrutture critiche nazionali sembrano aver trovato nuova linfa e alte capacità di impatto e di successo (si vedano, di seguito, le schede su Russia e Stati Uniti).

ISRAELE

Il governo israeliano ha da tempo puntato gran parte dell'attenzione istituzionale sulle questioni relative alla 'sicurezza cibernetica', sia sotto il profilo militare e di intelligence per la salvaguardia dei propri interessi strategici, che come veicolo e volano dello sviluppo economico. Nell'arco di soli tre anni, Israele – attraverso il suo "CyberParco" di Be'er Sheva completamente dedicato alla sviluppo della cyber-security – ha acquisito in questo settore una posizione dominante a livello globale. Stando alle ultime stime ufficiali, infatti, oggi Israele ospita sul suo territorio oltre 300 aziende che fanno della cyber-security il proprio core business. Esse, peraltro, esportano annualmente servizi e tecnologie per circa 6 miliardi di dollari e rappresentano il 20% dell'investimento privato mondiale nel settore. Questi numeri e la loro costante crescita hanno portato a gennaio il Primo Ministro Netanyahu a spingere per la trasformazione del "CyberParco" di Be'er Sheva non più solo come punto di riferimento della cyber-security a livello nazionale, ma di provare ad estendere il progetto anche a livello globale. Ciò, complice la distrazione dei governi europei verso gli evidenti benefici di simili iniziative e nonostante un progetto analogo a quello israeliano siano già stato delineato, ad esempio, proprio in Italia.

In una recente conferenza a Tel Aviv,

inoltre, il Primo Ministro Netanyahu ha anche preannunciato l'imminente pubblicazione di alcune norme volte a regolamentare l'esportazione di prodotti per la cyber-security da parte delle aziende israeliane. L'intento appare essere quello d'inserirsi nel medesimo solco tracciato dagli Stati Uniti attraverso l'estensione dell'accordo Wassenaar all'esportazione di tecnologie e di software utili alla sorveglianza e all'hacking di sistemi informatici. Accordo che, peraltro, proprio agli inizi di quest'anno ha visto un riaccendersi delle polemiche politiche negli Stati Uniti, al fine di ottenere nuove modifiche e maggiori aperture per le aziende. Medesime polemiche che, al momento, infiammano anche il dibattito politico israeliano.

RUSSIA

Pochi giorni prima delle festività natalizie dello scorso anno, il governo russo è nuovamente balzato agli onori della cronaca a seguito di un suo possibile coinvolgimento in un attacco informatico coordinato contro alcune infrastrutture energetiche site sul territorio ucraino. Il 23 dicembre 2015, infatti, le compagnie energetiche PrykarpattiaOblEnergo e KyivOblEnergo, deputate ad erogare energia elettrica nella regione occidentale dell'Ucraina, hanno pubblicamente affermato di aver subìto un attacco informatico ai sistemi di gestione di numerose sottostazioni elettriche, causando un blackout esteso e prolungato in gran parte della regione. Seppure approfondire i dettagli tecnici dell'attacco non è lo scopo primario, occorre comunque evidenziare come il *Trojan* utilizzato, il famoso "BlackEnergy" (la cui prima versione fu impiegata nei celeberrimi attacchi DDoS del 2008 contro la Georgia), sia stato inoculato attraverso un mero *file* Microsoft Word capace di sfruttare un ben noto *bug* del 2014 nella gestione delle *macro* da parte di Office (per la precisione il CVE-2014-4114). Un metodo, quindi, assolutamente poco innovativo sul piano tecnico, ma anzi particolarmente conosciuto e già ampiamente utilizzato.


12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

Ciò che più interessa sul piano dell'analisi in un'ottica di sicurezza nazionale, però, è certamente la crescente attenzione che i sistemi ICS/SCADA stanno avendo – in particolar modo dal 2013 – da parte degli sviluppatori di *malware*. Un settore, quello delle infrastrutture critiche, particolarmente delicato per la sua caratteristica, in caso di incidente, di produrre effetti direttamente nel mondo fisico – come nel caso del blackout in Ucraina – e dove la crescente "necessità" d'interconnessione tra i sistemi, unita alla mancanza delle più elementari misure di sicurezza nelle tecnologie e nei protocolli utilizzati, rappresentano senz'altro una vera e propria spina nel fianco per ogni governo.

Sotto altro profilo, invece, occorre evidenziare come, a dispetto dei proclami giornalistici su un'ipotetica "cyber-war" in atto da tempo tra Russia e Ucraina, nessuno dei due attori fino a questo momento si era realmente adoperato per sfruttare le tecnologie e la rete Internet per confezionare attacchi informatici classificabili come atti di *cyber-warfare*. Men che mai attacchi, come quello subìto dall'Ucraina, capaci peraltro di produrre effetti diretti sulla popolazione. Questo blackout, pertanto, rappresenta sicuramente un evento da seguire nei suoi sviluppi con estrema attenzione. Infatti, qualora col tempo fosse provato il coinvolgimento del governo russo – assolutamente teorico al momento – questo attacco informatico potrebbe essere classificato sotto il punto di vista del diritto internazionale quanto meno come "uso della forza", il cui divie-

to è sancito dall'art. 2, § 4, della Carta ONU, con tutte le conseguenze che ne deriverebbero per la Russia, sia sotto il profilo dei rapporti internazionali, che sotto il punto di vista della possibilità di reazione legittima a questo attacco da parte dell'Ucraina.

STATI UNITI

Sulla scia delle garanzie giuridiche previste all'interno del capitolo "*Cyber Operations*" del mastodontico "*Law of War Manual*" pubblicato a giugno del 2015, lo U.S. Cyber Command si appresta ad appaltare alle aziende private un progetto da oltre 450 milioni di dollari. L'obiettivo è quello di vedersi affiancato – nell'arco dei prossimi 5 anni – nello sviluppo dei "*Cyberspace Operations Support Services*" utili al Pentagono per proiettare forza anche nel cosiddetto quinto dominio della conflittualità, il cyber-spazio appunto. A tal fine, lo U.S. Cyber Command punta ad avere entro la fine di quest'anno ben 6.200 militari specializzati in operazioni nel e attraverso il cyber-spazio. Tuttavia, ciò che più rileva di questo progetto è senz'altro l'intenzione di richiedere alla società vincitrice dell'appalto anche lo sviluppo e la distribuzione di cyber-armi e di far ciò in cooperazione con le agenzie di intelligence americane. In particolare, la bozza del contratto prevede che la società supporti tecnicamente lo U.S. Cyber Command nel pianificare, coordinare e sincronizzare sia le operazioni militari difensive, che quelle offensive attuate per mezzo del cyber-spazio, nonché di consigliare, sviluppare, valutare, analizzare e integrare le cyber-armi all'interno di questo genere di operazioni. Appare evidente, quindi, come il governo americano lavori ormai da tempo e senza sosta per consolidare la propria *leadership* internazionale nelle attività militari nel e attraverso il cyber-spazio, spingendo sempre più verso una postura marcatamente offensiva, utile già oggi ai fini del rafforzamento della loro strategia di deterrenza.

Ciò, peraltro, si raccorda perfettamente con la proposta di finanziamento per il 2017 che il Pentagono ha formulato agli inizi di febbraio. Solo per il settore della *cyber-security*, infatti, la richiesta è di 7 miliardi di dollari per il prossimo anno (circa un miliardo in più rispetto alle richieste per il 2016) e di 35 miliardi di dollari per i prossimi 5 anni da destinare alla protezione delle infrastrutture militari, ma anche – si legge esplicitamente nella richiesta – per accelerare lo sviluppo delle capacità offensive nel e attraverso il cyber-spazio. ■

Un anno in retrospettiva: le minacce cyber del 2015

In qualsiasi disciplina o attività, le prime settimane di ogni nuovo anno sono il momento d'elezione per fermarsi un attimo a fare il punto della situazione e tirare le somme su ciò che è successo nei precedenti dodici mesi. Valutare lo stato delle cose a mente fredda e ad intervalli prefissati aiuta infatti a rendersi meglio conto dei trend di lungo respiro, e quindi anche a farsi un'idea di cosa succederà nel prossimo futuro e di come ci si potrebbe preparare a ciò che verrà.

La cybersecurity non fa eccezione, ed infatti sono molti i vendor e i ricercatori che al cambio d'anno ci propongono, ciascuno dal proprio personale punto di vista, le loro considerazioni sui fenomeni rilevanti che hanno caratterizzato l'anno appena terminato; e magari anche le proprie anticipazioni su ciò che si aspettano da quello appena iniziato, alla luce delle tendenze analizzate.

Fra tutti i rapporti del genere spicca da oramai quattro anni quello pubblicato da ENISA, l'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione, sul cosiddetto "panorama delle minacce". Stante infatti la particolare posizione "super partes" e strategica del-

Corrado Giustozzi: Attivo da oltre trent'anni nella cybersecurity come consulente, docente e divulgatore. Membro da tre mandati del Permanent Stakeholders' Group dell'Agenzia dell'Unione Europea per la Sicurezza delle Reti e delle Informazioni (ENISA), esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT della Pubblica Amministrazione, componente del Consiglio direttivo di Clusit.
Collabora da anni con diverse forze dell'ordine e con l'Ufficio delle Nazioni Unite per il controllo della droga e la prevenzione del crimine (UNODC) nel contrasto al cybercrime ed al cyberterrorismo internazionali.
Membro di varie associazioni scientifiche e tecniche, componente di molteplici comitati scientifici, docente presso varie Università, svolge da sempre un'intensa attività di divulgazione culturale dei temi cyber tenendo frequentemente conferenze e seminari specialistici. Giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), ha al suo attivo oltre mille articoli e quattro libri.

l'Agenzia, che traguarda tutto il mondo con particolare riguardo all'Unione Europea e riceve dati di prima mano da alcuni specifici settori di mercato in tutti gli Stati membri, questo lavoro offre una visione estremamente ampia ed accurata dei fenomeni legati al mondo del rischio cyber, identificando e catalogando le minacce più rilevanti, le vulnerabilità da esse sfruttate e le modalità con cui esse vengono impiegate dalla criminalità e dalle altre forze che "giocano contro".

IL RAPPORTO ETL 2015

Il rapporto "ENISA Threat Landscape 2015", pubblicato a fine gennaio, è il quarto di quella che è oramai diventata una serie tradizionale. Come di consueto si focalizza sugli eventi cyber più significativi occorsi nei dodici mesi precedenti, categorizzandoli per tipologia di minaccia. Ciascuna minaccia viene inoltre valutata secondo la sua rilevanza e soprattutto la sua diffusione, dando così origine ad una sorta di "hit parade" delle 15 principali minacce che vede ai primi posti della classifica quelle maggiormente diffuse o che hanno causato i maggiori danni. Ciascuna delle "top threats" risultanti viene inoltre confrontata con la sua posizione nel rapporto precedente, in modo da tracciarne anche l'andamento tendenziale e tentare di prevederne la possibile evoluzione.
In Figura 1 vediamo la tabella riassuntiva del rapporto di quest'anno, che riporta il raffronto tra le posizioni attuali e quelle dell'anno scorso. Per ciascuna delle minacce presentate viene indicato il trend di crescita relativo all'anno considerato, mentre l'indicatore nell'ultima colonna rappresenta l'eventuale spostamento della minaccia all'interno della classifica, rispetto quella dell'anno precedente. Si vede a colpo d'occhio che le cinque minacce più rilevanti sono rimaste sostanzialmente invariate fra 2014 e 2015, mentre al sesto e settimo posto si sono insidiate minacce che in precedenza erano state classificate più in bassso nella lista.
Oltre all'analisi dettagliate delle "top threats" il rapporto fornisce ulteriori interessanti considerazioni metodologiche, ad esempio proponendo nonché adottando una tassonomia per la classificazione dei rischi sviluppata *ad hoc* come armonizzazione di quanto già esistente in letteratura. Infine vengono illu-

CORRADO GIUSTOZZI

Membro del Permanent Stakeholders' Group di ENISA ed esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT-PA

Top Threats 2014	Assessed Trends 2013	Top Threats 2015	Assessed Trends 2014	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	➲	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	➲	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
11. Insider threat	➲	11. Data breaches	➲	↓
12. Information leakage	↑	12. Identity theft	➲	↑
13. Identity theft/fraud	↑	13. Information leakage	↑	↓
14. Cyber espionage	↑	14. Ransomware	↑	↑
15. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

strate le "lesson learned", ossia cosa abbiamo imparato dagli incidenti occorsi, e prodotte raccomandazioni indirizzate ai decisori in ambito politico, aziendale e della ricerca.
In questo articolo riportiamo una rapida overview delle principali minacce poste da Enisa ai vertici della classifica, rimandando alla lettura del report originale[1] tutti coloro che fossero interessati ad approfondire gli ulteriori numerosi appprofondimenti che vi si trovano.

MALWARE

Come già accennato, nel 2015 il malware si è confermato al primo posto tra le minacce cyber, così come già era successo l'anno precedente. Particolarmente rilevante la presenza di malware specifico per dspositivi mobili (smartphone e tablet), cresciuto di oltre il 50% rispetto al 2014.
Fra gli aspetti interessanti che il report evidenzia va menzionato il ritorno di tecniche di infezione risalenti a vent'anni fa e date per scomparse, quali documenti Office che, mediante macro (in Visual Basic), scaricano il malware sul PC dell'utente e lo installano. Due importanti casi di questa tecnica "vintage" sono Duku 2 e Equation Group.
Un'altra caratteristice interessante rilevata da ENISA è lo spostamento del vettore di diffusione dall'attachment di email alla URL malevola, conseguente all'aumento di infezioni veicolate tramite profili o messaggi sui social network.
Interessante infine sottolineare come la Russia da sola ospiti la metà dei siti di risorse di malware online del mondo, con gli USA al secondo posto ma ben distaccati (12%) e tre Paesi europei a seguire (Olanda, Germania e Francia).

WEB BASED ATTACKS

Gli attacchi web-based sono quelli che sfruttano il Web, sia lato server che lato client, come mezzo per rilevare vulnerabilità ed installare malware. Essi comprendono ad esempio tecniche come URL malevole, pagine Web compromesse, exploit sul browser eccetera.
Una novità del 2015 è stato l'uso di plugin specializzati, che vengono installati nei browser da pacchetti software indesiderati, e sono utilizzati per inviare spam o mostrare pubblicità non richieste e non eliminabili. Al fine di sfuggire il rilevamento questi plugin usano casualmente circa 400 nomi e 500 domini.
In generale nel corso del 2015 sono state identificate da vari CERT circa 58.000 nuove URL malevole al giorno, ossia oltre venti milioni nell'anno, il che rende particolarmente oneroso il loro blocco mediante strumenti convenzionali (blacklist), che sono tuttavia praticamente l'unica forma di contrasto disponibile.

WEB APPLICATION ATTACKS

Sì, i "soliti" vecchi cross-site scripting e SQL injection, che apparentemente erano diminuiti nel 2014, sono tornati più vispi di prima
La stessa vulnerabilità Shellshock, apparsa e ben studiata nel 2014, è ritornata prepotentemente alla ribalta risultando responsabile da sola di oltre il 40% degli attacchi alle web application.

BOTNETS

Le botnet rimangono un fenomeno estremamente rilevante, anche se le loro modalità di azione sta cambiando. Ad esempio, in seguito del famoso takedown dela rete Gameover Zeus, ne è stata rilevata una nuova versione che non sfrutta più i protocolli P2P, un cui bug era stato sfruttato dalle forze di polizia proprio per smantellare la rete precedente.
È anche in atto un riposizionamento dei centri di comando e controllo (C&C) da server fisici infettati con malware a server virtuali, più facili da gestire dinamicamente e meno esposti a rischi per il botmaster. Sono inoltre state osservate le prime botnet formate da dispositivi IP, l'inizio di quella che si teme sarà il maggior problema della prossima

[1] Il rapporto è liberamente scaricabile da: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015/etl2015/at_download/fullReport

Internet of Things.
Globalmente nel corso del 2015 sono stati identificati dai 600 ai 1.000 C&C, ciascuno dei quali responsabile di alcune centinaia di migliaia di macchine zombie. L'utilizzo tipico è stato il noleggio delle reti per attività di Cybercrime-As-A-Service, in particolare per sferrare attacchi di Denial of Service massivo (DDoS) a tariffe di mercato variabili fra i 20 e i 40 dollari l'ora.
Una rete in particolare, denominata Nidol, si è resa da sola responsabile del 60% di tutti gli attacchi applicativi del 2015.

DENIAL OF SERVICE

Gli attacchi di tipo Denial od Service hanno visto nel 2015 un consistente incremento sia in termini di qualità che in termini di quantità rispetto all'anno precedente. In particolare il numero complessivo degli attacchi è aumentato del 130%, quello degli attacchi a livello applicativo del 120%, quello degli attacchi a livello di infrastruttura del 130%, quello degli attacchi con volume superiore ai 100 gbps del 100%. È inoltre stata registrata la tendenza ad abbandonare i tradizionali sistemi usati per gli attacchi, tipicamente macchine server di elevata potenza, in favore di dispositivi economici, meno potenti ma più diffusi quali i router casalinghi, sfruttando attacchi basati sul protocollo UPnP.
Nel corsso del 2015 sono anche aumentati i casi di attacchi DDoS usati come fonte di lucro per la criminalità, mediante un meccanismo che vede dapprima lanciare un attacco massiccio contro la vittima e successivamente chiedere il pagamento di un riscatto per farlo cessare.

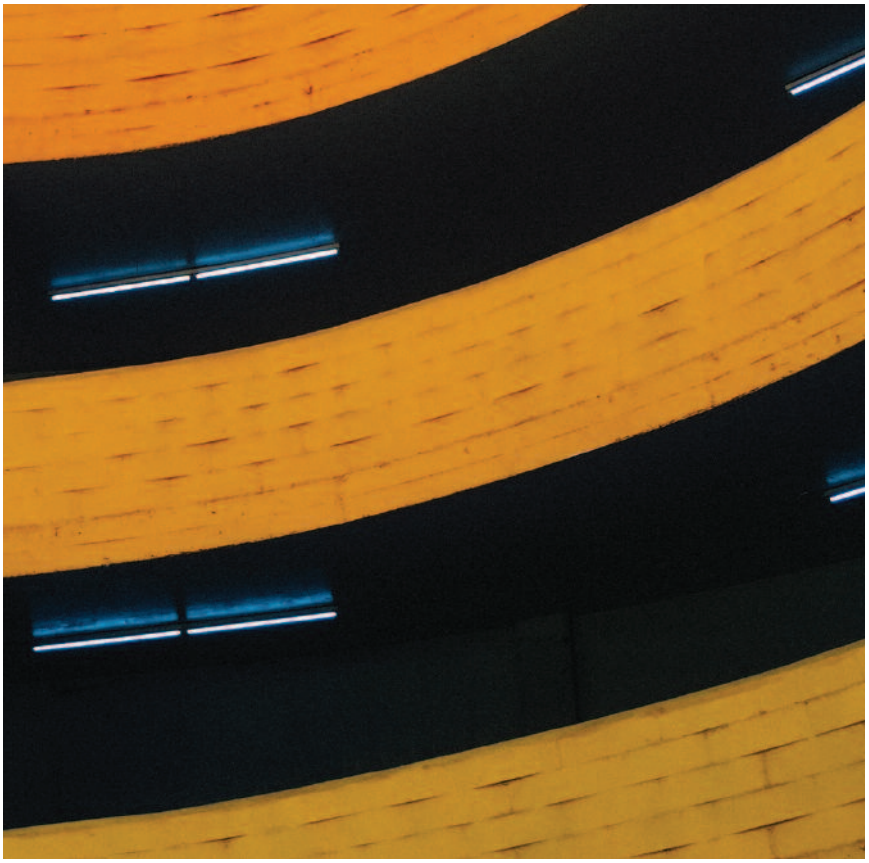
CONSIDERAZIONI SU ALTRE MINACCE

Per quanto riguarda le rimanenti posizioni della top 15, non potendo commentarle tutte una ad una è interessante notare almeno le categorie in ascesa: *phisical damage/theft/loss* (danno, furto o perdita fisica), *insider threat* (minaccia interna), *identity theft* (furto d'identità) e *ransomware* (malware che cifra i dati e chiede il riscatto per decifrarli).
Il furto fisico di apparati, per quanto banale, rimane una delle più importanti cause di perdita (e quindi spesso di diffusione) di dati riservati. La maggior parte degli episodi (55%) avviene sul luogo di lavoro, ma oltre il 22% riguarda o coinvolge materiale presente a bordo di autoveicoli. In generale il furto di dispositivi è il danno più probabile per un'azienda o organizzazione, prima ancora dell'intrusione o del Denial of Service!
La minaccia dall'interno, sia deliberata che non intenzionale, è un grande classico che non passa mai di moda: circa un terzo di tutti gli incidenti può essere ricondotto ad attività di questo tipo. Tuttavia un sondaggio ha mostrato che il 75% delle aziende interessate ha preferito risolvere l'incidente direttamente senza denunciarlo alla polizia.
Il furto d'identità è un caso particolare di furto d'informazioni che riguarda dati relativi all'identità personale, i quali possono avere un valore immediato sul mercato criminale. Gli episodi registrati nel 2015 hanno riguardato soprattutto dati sanitari, che da soli hanno costituito circa un terzo dei casi totali.
Il ransomware è sicuramente il fenomeno che più ha caratterizzato il 2015: in effetti il numero di episodi registrati è più che raddoppiato rispetto all'anno precedente, raggiungendo il suo attuale massimo storico, mentre il numero di nuovi tipi o varianti è più che quaduplicato.

CONCLUSIONI

Gli analisti di ENISA notano a margine che nel 2015 non ci sono stati eventi eclatanti sul fronte cyber, come lo furono ad esempio le rivelazioni Snowden l'anno passato. Questa apparente tranquillità ha permesso ai cattivi di sviluppare con maggior cura e calma i propri strumenti di attacco, migliorandoli in qualità ed efficienza e di fatto aumentando silenziosamente ma sistematicamente il loro livello di minaccia.
D'altro canto l'analisi degli incidenti mostra che nella grande maggioranza dei casi non vi erano neppure le più basilari misure di protezione, o quelle che c'erano non hanno funzionato come ci si attendeva. Il problema della prevenzione ruota attorno alla preparazione ed alla consapevolezza degli utenti e delle organizzazioni, e sarebbe utile definire una baseline comune di misure minime di sicurezza per ottenere almeno un livello di base uguale per tutti. ■

Contromisure dinamiche: perché, quando e soprattutto come



Continuiamo la presentazione dei vantaggi di una metodologia che permetta di predire, in modo quantitativo e ripetibile la capacità di un sistema di resistere agli attacchi. Il tema di quest'articolo sono le contromisure, quelle permanenti e quelle dinamiche. Una contromisura è una modifica al sistema o al modo in cui il sistema è utilizzato che riduce la probabilità di successo di un attacco semplice. Un attacco semplice è il singolo passo della privilege escalation che un attaccante deve realizzare per raggiungere il proprio obiettivo. Una contromisura permanente modifica uno o più componenti del sistema in modo definitivo. Tipici esempi sono l'applicazione di una patch per rimuovere una vulnerabilità in un modulo software, la segmentazione di una singola rete in più reti separate da un firewall o l'esecuzione di alcuni moduli su macchine virtuali diverse per meglio confinare gli attacchi. Contromisure di questo tipo devono essere valutate attentamente per garantire che il loro costo, spesso elevato, abbia come controparte un aumento della robustezza del sistema. Come già discusso nel precedente articolo sulle "contromisure benefiche"[1], occorre infatti evitare la

situazione paradossale di investire in una contromisura che aumenti la probabilità di successo dell'attaccante. Oltre alle contromisure permanenti, è possibile adottare anche quelle dinamiche. Una contromisura dinamica cambia la struttura del sistema ma per un intervallo di tempo limitato, tipicamente fino al termine dell'attacco. Tipici esempi sono la modifica delle regole di routing per difendersi da un DDOS o l'interruzione di alcuni collegamenti. In casi estremi si possono anche spegnere alcuni nodi o a disconnetterli dalla rete per creare un air gap. Il vantaggio delle contromisure temporanee è che possono essere molto severe visto che sono applicate per un tempo limitato. Il vero problema nasce però se pensiamo ai componenti del sistema che devono decidere quando applicarle. Consideriamo ad esempio la drastica contromisura che prevede di spegnere un nodo. E' ovvio che il nodo debba essere spento prima dell'inizio dell'attacco perché, visti i tempi tipici di un attacco adottare la contromisura dopo l'inizio dell'attacco può essere del tutto inutile.

E' anche altrettanto ovvio che visti i tempi degli attacchi informatici, la decisione non può essere delegata ad un essere umano. Per risolvere il problema dobbiamo ritornare ad uno dei concetti che stanno alla base del nostro approccio, la necessità di prevedere i possibili comportamenti degli attaccanti come chiave per garantire una difesa efficace e conveniente. Vediamo come questa previsione sia possibile quando di utilizza la metodologia Haruspex.

Haruspex assume che il sistema sia attaccato da uno o più agenti intelligenti che hanno come obiettivo il possesso di uno o più privilegi in modo da controllare uno o più moduli del sistema. Ad esempio, un agente che voglia rubare delle informazioni è interessato a controllare alcuni database e dei nodi che gli permettano di esfiltrare le informazioni. Invece, un attaccante interessato a sabotare un impianto industriale è interessato a controllare alcuni dei PLC che interfacciano il sistema di controllo e l'impianto stesso. I vari agenti raggiungono un loro obiettivo mediante privilege escalation ottenuta grazie ad una catena di attacchi elementari. Ogni attacco elementare aumenta i privilegi dell'agente e sfrutta una

1 Si veda il numero di ICT Security del Maggio 2015

FABRIZIO BAIARDI

Full Professor
Department of Computer Science
Università di Pisa

J. LIPILINI

F. TONELLI

Dipartimento di Informatica, Università di Pisa, Italia

o più vulnerabilità o weakness del sistema. Se l'attaccante riesce ad eseguire tutti gli attacchi della catena allora raggiunge il suo obiettivo. Possono esistere catene diverse per uno stesso obiettivo, queste catene possono essere viste come strade diverse che l'agente percorre nel sistema target. L'intelligenza dell'attaccante implica un minimizzazione dello sforzo, e quindi la scelta della catena più breve e più conveniente. La stessa intelligenza permette all'attaccante di cambiare la catena che sta realizzando in base alle contromisure adottate. Gli strumenti Haruspex permettono di costruire più modelli, uno del sistema da analizzare ed uno per ogni agente che può attaccare il sistema. Il modello del sistema descrive le due informazioni fondamentali per capire come il sistema può essere attaccato e cioè le vulnerabilità dei moduli del sistema, l'allocazione dei moduli ai vari nodi di elaborazione del sistema e le connessioni tra questi nodi. L'informazione sulle vulnerabilità permette di scoprire gli attacchi elementari che gli agenti possono eseguire, le risorse che tali attacchi richiedono e la loro probabilità di successo. La conoscenza delle connessioni tra i nodi permette di capire come gli agenti possano estendere il loro controllo da un nodo ad un altro. Il modello dell'agente è formato da un insieme di attributi che descrivono i suoi obiettivi, le sue capacità e le sue preferenze. Ad esempio, possiamo modellare agenti che sanno costruire degli exploit oppure che sanno solo usare gli exploit già pubblici. Un agente potrebbe preferire raccogliere una grande quantità di informazione per eseguire poi attacchi mirati, mentre potrebbero raccogliere il minimo di informazioni ed eseguire un attacco il prima possibile.

Costruiti il modello del sistema e quelli degli agenti che lo attaccano, altri strumenti Haruspex li eseguono in modo interattivo. Nell'esecuzione, il modello di un agente interagisce con quello del sistema, scegliendo ed eseguendo i vari attacchi possibili in base agli obiettivi dell'agente, alle sue capacità ed alle sue preferenze. L'esecuzione tiene anche conto del tempo che l'agente deve spendere per acquisire le informazioni necessarie per scegliere il prossimo attacco da eseguire. Sono anche possibili interazioni tra i modelli dei vari agenti per rappresentare lo scambio di informazioni ed i diritti. La simulazione passo passo del comportamento degli agenti permette di non dover ricostruire a priori tutte le possibili catene che un agente può scegliere evitando una esplosione esponenziale delle alternative da considerare.
Questa esplosione ha fino ad ora impedito di utilizzare approcci basati su attack graph o su altri formalismi che richiedano di modellare inizialmente tutte le possibili catene di un agente.

La singola esecuzione dei vari modelli restituisce un insieme di informazioni sul comportamento del sistema e degli agenti. Per quel che interessa in questo articolo, le informazioni di interesse sono la sequenza degli attacchi di ogni agente e l'obiettivo eventualmente raggiunto. Una sequenza è diversa da una catena, perché un agente può scegliere inizialmente una catena e poi cambiare tale scelta a causa del fallimento ripetuto di alcuni attacchi. La sequenza comprende eventuali ripetizioni e permette di dedurre altre informazioni quali il numero di attacchi diversi o il tempo impegnato per raggiungere un obiettivo. La singola esecuzione restituisce informazioni solo parziali visti fattori stocastici che la influenzano. Il principale di questi fattori è il successo o il fallimento di un attacco che influenza la scelta degli attacchi successivi dell'agente. Per tener conto dei fattori stocastici, e vista l'impossibilità di analizzare a priori tutte le alternative che essi possono generare, Haruspex applica il metodo Monte Carlo ed esegue esperimenti. Ogni esperimento comprende più esecuzioni indipendenti del modelli del sistema e degli agenti e restituisce un campione statistico sui vari eventi che permette di calcolare le statistiche di interesse quali tempo minimo, massimo e medio per raggiungere un certo obiettivo. La possibilità di calcolare tempi minimi e massimi per raggiungere un obiettivo è di particolare rilevanza perché il tempo medio è spesso una informazione troppo rozza per una valutazione realistica della robustezza di un sistema.
Per citare un antico proverbio, "Molte persone alte due metri sono morte attraversando un fiume profondo in media un metro". Tipicamente, il nu-

mero di esecuzioni necessarie per calcolare statistiche con una confidenza superiore al 95% varia da 10.000 a 50.000. Questo numero cresce con il numero di catene diverse a disposizione di un agente. Tra tutti i valori restituiti dal metodo Monte Carlo, quello che ci interessa qui è un database per ogni agente con tutte le sequenze di attacchi che l'agente stesso ha eseguito nelle varie esecuzioni.

E' estremamente interessante analizzare il database di ogni agente perché ciò permette di scoprire informazioni fondamentali per la difesa del sistema.
Ad esempio, la percentuale di esecuzioni che restituiscono la stessa sequenza è una accurata approssimazione della probabilità che l'agente scelga la sequenza stessa. Analisi più sofisticate permettono di scoprire le catene eseguite in ogni esecuzione e di come l'agente sia passato da una catena ad un altra. Il cambio di strategia dell'agente è dovuto, in genere, al fallimento ripetuto di un attacco o alla scoperta di una migliore catena. Altre analisi permettono di correlare i vari attacchi di uno stesso agente e permettono di scoprire, ad esempio, che ogni volta che un agente attacca un nodo n_1 poi attacca un nodo n_2. Di particolare interesse sono gli m-gram cioè le sottosequenze di m attacchi presenti nelle varie sequenze di un agente e gli m-gram unici, quelli che compaiono cioè nel database di un solo agente. Gli m-gram unici, se esistono, possono essere visti come una firma che permette di riconoscere l'agente.

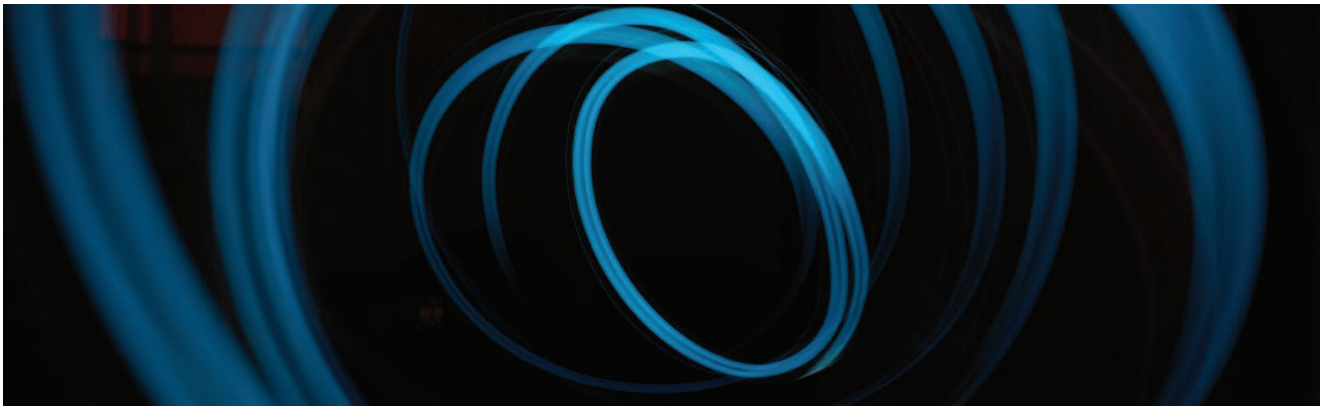
Per illustrare la relazione tra i database dei vari attaccanti e le contromisure dinamiche occorre supporre che nel sistema da proteggere esista un sistema di intrusion detection con dei sensori per il monitoraggio in tempo reale delle intrusioni. Per rilevare gli attacchi i sensori possono utilizzare le *signature* dei vari attacchi. Individuata una *signature* nel flusso delle informazioni, i sensori possono risalire immediatamente all'attacco che essa identifica. I sensori scoprono gli attacchi eseguiti contro il sistema ad un certo istante ed il sistema di monitoraggio ricostruisce e rende disponibile uno stream con la sequenza degli attacchi eseguiti. Il sistema di monitoraggio inserisce un nuovo attacco nello stream ogni volta che un sensore rileva un attacco. Il sistema di monitoraggio ha un ruolo fondamentale in tutti quei sistemi in cui alcuni agenti possono raggiungere i loro obiettivi perché non sono state adottate delle contromisure permanenti che garantiscano di bloccare ogni catena che permette ad un agente di raggiungere i suoi obiettivi. Notiamo che ciò non richiede di adottare delle contromisure permanenti che impediscano qualsiasi attacco perché questo potrebbe non essere conveniente. In generale è sufficiente bloccare un attacco di ogni catena che permetta ad un agente di raggiungere un obiettivo. Bloccando un attacco che appare in catene diverse si diminuisce il costo delle contromisure e si aumenta il ritorno dell'investimento. Quindi in generale gli agenti sono sempre in grado di eseguire alcuni attacchi ma in alcuni sistemi non possono raggiungere i loro obiettivi, o possono farlo con una probabilità trascurabile, mentre in altri li raggiungono con una probabilità elevata perché non è possibile o conveniente bloccare tutte le catene. Contromisure dinamiche sono utili solo nel secondo caso.

Supponiamo di dover aumentare la robustezza mediante contromisure dinamiche e di averne individuato alcune convenienti ed efficaci per il nostro sistema. Ad esempio, è possibile adottare una di tali contromisure per un attacco *Att* ma, come già detto, essa deve essere adottata prima che un agente esegua *Att*. Vediamo come si può risolvere il problema mediante uno strumento Haruspex, l'intrusion prevention system predittivo o *IPSpred*, che integra le informazioni nello stream restituito dal sistema di monitoraggio con quelle nei vari database degli agenti prodotti da un esperimento Haruspex. *IPSpred* può attivare la contromisura per *Att* non appena raggiunge una ragionevole certezza che esso sarà eseguito dall'agente che sta attaccando il sistema. Inizialmente, *IPSpred* analizza tutti i database e seleziona per ognuno il sottoinsieme con tutte le sequenze in cui compare *Att*. Di ognuna di tali sequenze, *IPSpred* conosce anche la probabilità. Ogni volta che lo stream degli attacchi eseguiti viene esteso con un nuovo attacco, *IPSpred* esamina quali sequenze sono compatibili con la sequenza *st* restituita dallo stream. Una sequenza è compatibile se *st* è un suo prefisso, ovvero se essa inizia con *st*. Tutte le sequenze non compatibili non sono considerate quando un nuovo elemento viene inserito nello stream. Se, ad un certo istante, non esistono sequenze compatibili, allora la sequenza dell'attaccante non comprenderà *Att* e *IPSpred* termina la sua analisi che potrà riprendere in presenza di un nuovo attaccante. *IPSpred* scopre un nuovo attaccante quando l'ultimo attacco inserito nello stream è quello iniziale di una sequenza di un qualche agente. Supponiamo invece che esistano sequenze compatibili. Ogni agente nel cui database compaiano sequenze compatibili può eseguire *Att* con una probabilità che dipende dalla distanza media tra l'ultimo attacco eseguito ed *Att* nelle varie sequenze. Chiariamo il punto con un esempio.
Supponiamo nel database di un solo agente ci siano due sequenze compatibili. Nella prima mancano ancora d_1 attacchi mentre nella seconda ne mancano ancora d_2. Siano p_1 e p_2 le probabilità delle due sequenze. Quindi la distanza media che separa il sistema da Att è proporzionale a $(d_1 \cdot p_1 + d_2 \cdot p_2)/(p_1 + p_2)$ e la probabilità che esso sia eseguito è inversamente proporzionale a tale distanza. Infatti, più lontano nel futuro è l'attacco, più probabile è che intervenga qualche fattore che fermi l'attaccante. Viceversa, se la distanza è molto piccola, allora è estremamente improbabile che l'attaccante desista. La soglia sulla distanza al disotto della quale *IPSpred* adotta la contromisura dipende dalla tolleranza al rischio dell'owner del sistema. Minore la tolleranza, maggiore è la soglia sotto la quale la contromisura diventa effettiva. Nel caso di più agenti

con sequenze compatibili, possiamo avere una ulteriore media tra gli agenti oppure, se diffidiamo dei valori medi, possiamo considerare il caso pessimo ovvero l'agente con la distanza più bassa. Una analisi più sofisticata può considerare il tempo che ogni attacco richiede. Ovviamente, in questo caso *IPSpred* userà un tempo come soglia. Un ulteriore raffinamento può considerare l'agente al cui database appartengono le sequenze compatibili ed introdurre soglie specifiche per ogni agente.

Si possono facilmente immaginare le obiezioni dei nostri venticinque lettori. Ad esempio una molto seria riguarda eventuali falsi positivi o falsi negativi.
Ovvero il sistema di monitoraggio può segnalare attacchi che non sono stati eseguiti o non poter scoprire alcuni attacchi. Una prima risposta è che nessun sistema di prevenzione delle intrusioni può essere esente da errori nel caso di sensori non accurati. Si tratta in fondo di una ulteriore applicazione del noto principio "Garbage In, Garbage Out". Però anche in questo caso la metodologia Haruspex viene in soccorso. Infatti il verificarsi di falsi negativi o falsi positivi diventa critico nel momento in cui non esistono più sequenze compatibili perché ciò provoca la sospensione dell'analisi. Prima di decidere di sospendere l'analisi *IPSpred* verifica la possibilità dei due errori.
Ad esempio, per verificare la presenza di falsi positivi verifica se esiste una sequenza compatibile nel caso in cui si elimini un attacco dalla sequenza dello stream. Per verificare possibili falsi negativi, invece, *IPSpred* verifica l'esistenza di sequenze compatibili se si inserisce un ulteriore attacco nello stream. Se in uno o in entrambi i casi esistono sequenze compatibili allora l'analisi può proseguire. Ovviamente in questo caso si possono utilizzare soglie diverse per attivare le contromisure che tengano conto dell'assunzione sul falso positivo o negativo.
L'attivazione di contromisure dinamiche è solo uno dei possibili casi in cui si può integrare l'output del sistema di rilevazione delle intrusioni ed i database degli altri esempi. Un'altra applicazione che può essere utile è la previsione del prossimo attacco.
Dato lo stream degli attacchi rilevati, è possibile analizzare tutti i database degli agenti per scoprire le sequenze compatibili.
Analizzando le sequenze è possibile scoprire i prossimi passi di ogni agente e quindi costruire un insieme con i possibili attacchi successivi o con i possibili nodi che eseguono i moduli che sono il bersaglio di tali attacchi.
Ovviamente, inizialmente tali previsioni sono poco accurate perchè la cardinalità degli insiemi è elevata ed anche considerando le probabilità di ogni sequenza, quindi dei vari attacchi, non si ottengono risultati significativi. Ma dopo pochi passi l'accuratezza che si raggiunge è elevata. Ad esempio abbiamo applicato questo metodo al sistema di controllo di una centrale per la produzione di energia. I vari agenti hanno obiettivi che possono raggiungere eseguendo una decina di attacchi. In questo caso dopo al più 4 passi *IPSpred* identifica l'attaccante, l'obiettivo che sta cercando di ottenere e predice con una accuratezza molto elevata il prossimo nodo che attaccherà.

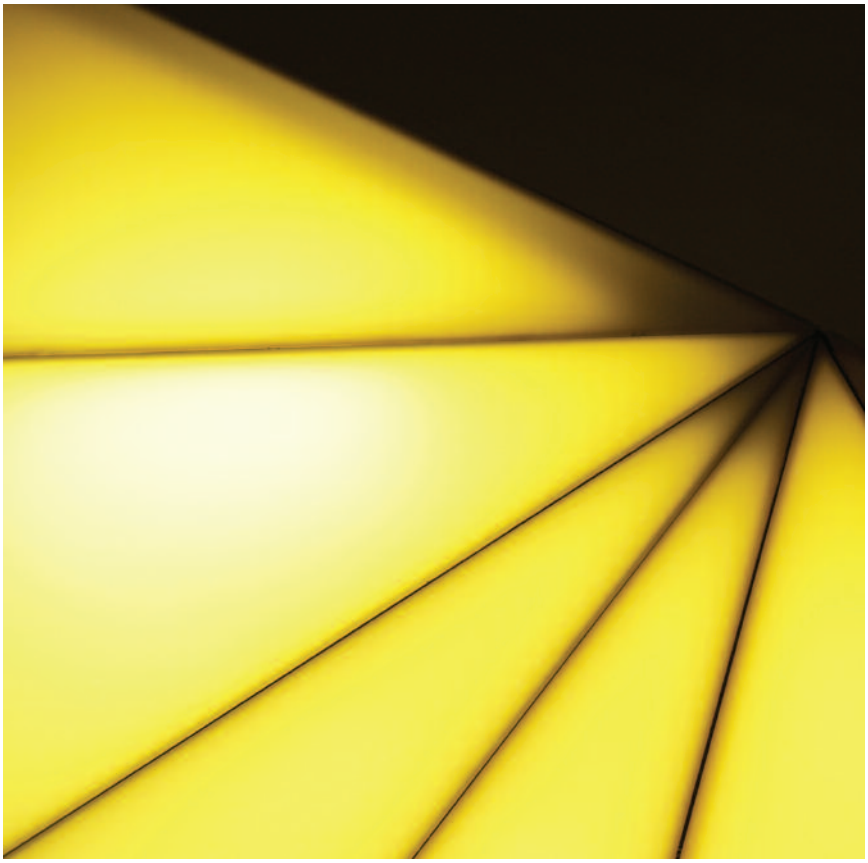
Infine l'ultima considerazione. E' possibile che il modello del sistema sia poco accurato e quindi gli attaccanti utilizzino contro il sistema sequenze che non abbiamo simulato? La risposta è ovviamente positiva. Gli strumenti Haruspex che costruiscono il modello del sistema assumono siano note tutte le vulnerabilità dei vari moduli che compongono il sistema. E' però ovviamente possibile che il sistema sia affetto da una o più *0-day* ovvero da vulnerabilità non ancora pubbliche. Se tali vulnerabilità non appaiono nelle posizioni iniziali di una sequenza è comunque probabile che esse siano state rese ininfluenti dalle contromisure permanenti che hanno bloccato delle catene. Comunque è sempre possibile che un attaccante che conosca tali vulnerabilità possa scegliere ed eseguire una sequenza diversa da quelle scoperte e restituite da un esperimento Haruspex.
Anche assumendo falsi positivi e/o negativi in questo caso nessuna delle sequenze restituite può essere compatibile. Questo è una situazione di rischio estremamente elevato che *IPSpred* riesce comunque a gestire. Infatti l'impossibilità di trovare sequenze compatibili anche assumendo falsi positivi o negativi rivela che il modello del sistema non è consistente rispetto agli attacchi che stanno avvenendo perchè l'attaccante che sta utilizzando 0-day. A seguito di questa scoperta *IPSpred* attiva le contromisure dinamiche più severe di cui dispone. ■



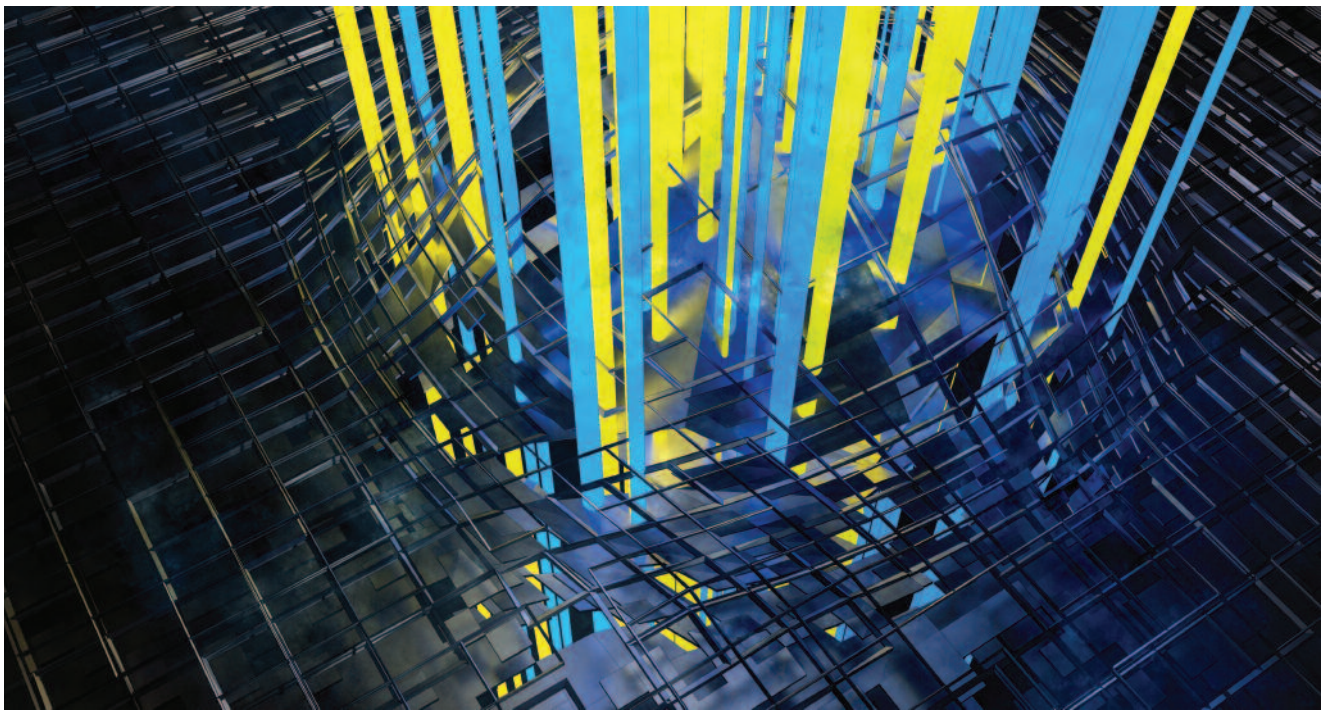

WATCHGUARD
DIMENSION
You have to SEE IT to believe it
Visibility
The only way to make smart decisions in the 21st Century
From the C-level office to network administration, business decisions need to be made at light speed – decisions that enhance productivity and profitability.
WatchGuard Dimension instantly turns raw network data into actionable security intelligence. It gives you the ability to see and understand how to protect your business, set tight security policy, and meet compliance mandates.
Go beyond reporting to the decision-making power of WatchGuard Dimension.
Pure visibility from any angle.
Email us today at italy@watchguard.com
Or call us: +39 066 0201 221
WatchGuard SMART SECURITY
www.watchguard.com

Il CERT Nazionale:

Campagne di Prevenzione e Reazione nel 2015



Il 2015 ha registrato un sensibile incremento delle attività del CERT Nazionale.
Se infatti nel corso della seconda parte del 2014 il CERT si era fortemente impegnato a stabilire i primi contatti con gli omologhi CERT internazionali, non solo a livello europeo, e a consolidare a livello nazionale le relazioni con i competenti soggetti pubblici ed il settore privato, durante tutto il 2015 la rete dei contatti ha avuto una consistente estensione, traducendosi in uno scambio crescente di informazioni che ha comportato la necessità di sviluppare strumenti opportuni per la loro gestione.
Il trend di crescita delle segnalazioni è dovuto, da un lato, all'estensione della rete dei contatti, a livello sia nazionale che internazionale, e dall'altro all'incremento del numero delle fonti di informazione che si traduce in nuovi servizi per gli operatori nazionali.
Inoltre, l'accreditamento ottenuto presso soggetti riconosciuti internazionalmente (Carnegie Mellon, Trusted Introducer) ha portato a nuovi contatti, soprattutto da parte di alcuni CERT internazionali.
Nell'ultimo periodo si registra un trend crescente per le segnalazioni



provenienti da soggetti privati, nazionali o internazionali; le segnalazioni dai CERT Europei ed internazionali si attestano, invece, intorno al 40% del totale.
Allo stato attuale è stato raggiunto dalle segnalazioni del CERT Nazionale un numero considerevole di Operatori/Internet Service Provider nazionali, di varia dimensione, corrispondente ad una copertura di più di 490 AS (Sistemi Autonomi) e più di 50 Milioni di indirizzi IP che coprono circa il 98% del totale di indirizzi afferenti ad AS italiani.
Nel dettaglio, i dati ricevuti direttamente da omologhi CERT nazionali ed internazionali e quelli desunti dalle nuove fonti di informazioni, tipicamente di tipo semi-aperte, con viste particolari riservate ai CERT nazionali, hanno portato complessivamente all'invio di 3.500 report corrispondenti ad oltre 750.000 eventi segnalati ai circa 375 Operatori/ISP entrati a far parte dei contatti del CERT Nazionale.
Un'attenzione particolare è stata dedicata alla predisposizione di campagne informative attingendo alle fonti più disparate, da quelle aperte, a quelle semi-aperte di security vendor che forniscono ai CERT Nazionali dati a livello Paese, a quelle chiuse rappresentate principalmente dagli omologhi CERT internazionali, a quelle interne, basate su dati desumibili dai propri sistemi.
Le campagne sono state divise in due categorie, quelle a carattere "preventivo" e quelle a carattere "reattivo": le prime legate a vulnerabilità rilevate in rete dovute a configurazioni errate o vulnerabilità intrinseche dei sistemi; le seconde legate a macchine risultate compromesse, generalmente appartenenti a botnet, rilevate attraverso il loro traffico anomalo registrato in rete.
In particolare alcune delle campagne "reattive" hanno riguardato siti web compromessi, relativamente ai quali il CERT Nazionale ha provveduto ad informare gli Operatori ed ISP coinvolti. La principale infezione segnalata è stata relativa alla spam-botnet nota come "stealrat". Sono stati circa 2.000 i siti web compromessi segnalati con l'ultima campagna di dicembre da questo sofisticato malware che, attraverso una tecnica basata su tre livelli di infezione (una prima macchina infetta appartenente ad una botnet, un primo web server che predispone lo spam, ed un secondo server

A CURA DI ISCOM

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Ministero dello Sviluppo Economico

che effettua l'attacco vero e proprio, per esempio ospitando un malware o una pagina di phishing o una qualsiasi altra pagina di atterraggio) , è in grado di eludere molti filtri anti-spam.
Altre campagne hanno invece riguardato la compromissione di singole macchine, che sono risultate appartenere a diverse botnet. Nel complesso queste campagne, avviate nel corso dell'anno, hanno riguardato le principali botnet note, con quasi 70.000 infezioni segnalate ai rispettivi Operatori/ISP, come riportato nel dettaglio.

Botnet	Macchine compromesse
Zeroaccess	30.500
Kelihos	11.000
Gozi	8.000
Ponmocup	5.000
Palevo	4.500
Tinba	4.000
Asprox	2.500
Dyre	2.000
Cutwail	1.500
Slenfbot	~ 900
Lethic	~ 150
Expiro	~ 100

La tipologia delle botnet è estremamente varia, così come i potenziali effetti sulla sicurezza della vittima e della rete nel suo complesso.
Molte di esse, come Cutwail, Kelihos, Asprox o Lethic, sono principalmente delle spam-botnet utilizzate, di fatto, per inviare spam di vario genere, fine a se stesso piuttosto che vettore di phishing o diffusione di altro malware più specifico. Altre sono dei veri e propri rootkit, mentre altre ancora sono pericolose stealer di credenziali, principalmente rivolte alle credenziali bancarie (Dyre e Tinba i più noti ed i più ricorrenti, nella categoria, anche nelle segnalazioni ricevute dal CERT Nazionale da fonti differenti).
Differente lo scopo delle campagne "preventive". Si tratta, di fatto, di informazioni pervenute al CERT Nazionale e relative a vulnerabilità scoperte in rete o a sistemi non correttamente configurati.
In particolare alcuni servizi lasciati non intenzionalmente "aperti" alla rete, possono rendere la macchina vettore di attacco DDoS verso terzi.
Le note tecniche utilizzate per attacchi DDoS Reflection and Amplification, congiuntamente alla possibilità di effettuare spoofing degli indirizzi IP delle macchine vittime, si arricchiscono sempre più di protocolli e servizi "aperti" che garantiscono un buon coefficiente di amplificazione.
Queste tecniche prevedono l'invio di richieste a macchine con determinati protocolli o servizi lasciati "aperti" in rete che prevedono risposte di lunghezza di ordini di grandezza superiori rispetto a quelli della richiesta ("amplification"). Attraverso tecniche di spoofing dell'indirizzo richiedente le risposte vengono inviate contemporaneamente alla macchina vittima, perpetrando così l'attacco, per saturazione di capacità del destinatario. Accanto ai protocolli e servizi, già usati in passato per attacchi anche di grande dimensioni, con alto coefficiente di amplificazione, come NTP (coefficiente di amplificazione pari a circa 500), Chargen (circa 350) e Quote of the Day (circa 140), nel corso dell'anno si è notato l'uso (con un picco registrato ad agosto) di attacchi che hanno utilizzato il servizio Portmapper, con un coefficiente di amplificazione pari a circa 30, ridotto, ma pur sempre interessante.
La necessità di utilizzare nuovi protocolli per gli attacchi deriva dal fatto che le configurazioni vengono generalmente corrette in seguito alla partecipazione della macchine ad attacchi DDoS. Per questo motivo il numero di macchine segnalate nelle varie campagne, che sono risultate essere in numero molto ridotto nel caso di servizi e protocolli "noti" (nell'ordine del migliaio, a livello italiano), per quest'ultimo caso, invece, sono state oltre 15.000.
Altre campagne hanno invece riguardato la diffusione di informazioni su macchine con servizi lasciati inavvertitamente "aperti" o con credenziali di accesso deboli. Tali situazioni espongono le macchine ad attacchi diretti oppure le trasformano in strumenti per altri attacchi come nel caso del DDoS. ■

KASPERSKY lab

THE POWER
OF PROTECTION

PROTEZIONE PRESENTE E SICUREZZA FUTURA

Soluzioni di sicurezza Kaspersky per la grande azienda

Un panorama di minacce sempre più sofisticate e complesse impone un approccio multilivello alla sicurezza IT, in cui una combinazione di tecnologie integrate fornisca funzionalità complete di rilevamento e protezione dalle minacce già conosciute... e da quelle ancora sconosciute.

Per tenere testa ai sofisticati livelli raggiunti oggi dalla cybercriminalità, sono necessari servizi di intelligence e tecnologie proattive per la sicurezza.
La nostra conoscenza di alcuni degli attacchi più sofisticati del mondo, insieme alla nostra capacità di rilevarli, ci consente di essere in grado di proteggere la vostra organizzazione oggi e nel futuro.

kaspersky.it/enterprise
#EnterpriseSec

KASPERSKY lab DISTRIBUTORE

TECHNE Security
www.technesecurity.it

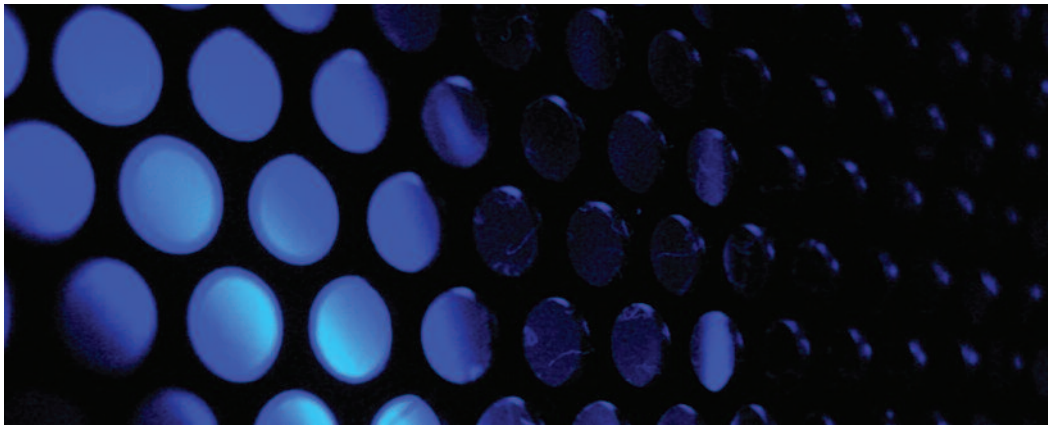
Cyber security: i trend del 2016

Martin McKeay, Senior Security Advocate di Akamai, analizza i trend sulla sicurezza informatica del 2015 e il loro sviluppo nel corso del 2016

È ormai un fatto assodato che la sicurezza informatica diventerà sempre più importante nei prossimi anni, guadagnando sempre più attenzione da parte del grande pubblico. Ci troviamo agli inizi di una serie imponente di cambiamenti che nessuno può prevedere con precisione. I professionisti della sicurezza si sono lamentati per anni del fatto che chi aveva il potere decisionale nelle imprese non dedicava sufficiente attenzione ai nostri allarmi, ma la situazione si sta velocemente trasformando, cogliendo molti impreparati e creando situazioni paradossali. Poiché nel 2015 si è dedicata moltissima attenzione al tema della sicurezza informatica, è utile cercare di delineare come alcune delle tendenze più significative del 2015 potrebbero evolvere negli anni a venire.

Martin McKeay, Senior Security Advocate di Akamai, analizza i trend sulla sicurezza informatica del 2015 e il loro sviluppo nel corso del 2016:

- **Crescerà la diffusione dei ricatti DDoS**
  Nel 2014 abbiamo visto comparire una nuova minaccia, DD4BC. Scomparsa nel 2015, è stata sostituita da Armada Collective. Entrambi i gruppi erano dediti all'invio di email con la richiesta di un pagamento in bitcoin con la minaccia, in caso contrario, di mettere fuori servizio il sito dell'azienda. Il loro successo ha portato Armada Collective a comportamenti sempre più aggressivi e alla nascita di un discreto numero di imitatori. Non c'è dubbio che il trend proseguirà nel 2016 e diventerà sempre più pericoloso poiché sempre più malintenzionati vedranno un potenziale in questo genere di ricatti.
- **L'Internet delle Cose sarà compromesso**
  L'Internet delle Cose rappresenta una vasta classe di tecnologie e prodotti, la maggior parte dei quali è stata progettata dedicando nulla più che un veloce pensiero alla sicurezza. Esempi recenti? Hello Barbie e la compromissione del produttore di giochi Vtech. Dobbiamo essere consapevoli che i dispositivi IdC raccolgono più informazioni sui loro proprietari di quanto essi possano immaginare e si tratta di dati molto preziosi. E anche se il dispositivo è perfettamente sicuro, i servizi che stanno dietro a quel dispositivo spesso lasciano molto a desiderare in termini di sicurezza. Ecco perché penso che assisteremo a un crescente numero di attacchi sia ai tool e ai giochi IdC sia alle aziende che raccolgono i nostri dati personali.
- **La sicurezza non aumenterà in modo significativo**
  Questo è un trend sul quale vorrei sbagliarmi ma quasi due decenni trascorsi ad occuparmi di sicurezza mi fanno pensare di aver ragione. Nonostante tutte le dichiarazioni dei fornitori di sicurezza che sostengono di disporre della soluzione a tutti i vostri problemi, un prodotto del genere non esiste. Dobbiamo invece convincerci che assisteremo a una lunga serie di piccoli miglioramenti alla sicurezza e che i progressi si misurano in decenni, non in anni. Le aziende troveranno metodi nuovi e più efficaci per proteggere i loro sistemi e a loro volta i criminali troveranno nuovi e più efficaci metodi per attaccare gli stessi sistemi. Col tempo e un po' alla volta, capiremo come costruire software e sistemi che siano intrinsecamente sicuri fin dalla nascita. Probabilmente nel 2016 ci sembrerà che la sicurezza peggiori, ma questo sarà un segnale del fatto che le



organizzazioni iniziano a riconoscere gli indicatori di una compromissione, più che di un reale peggioramento della sicurezza.

- **I governi avranno un impatto importante sulla sicurezza**
  La Cina ha sempre preteso di avere accesso a tutto il traffico sul suo Internet; la Russia ha varato una legge nel 2014 in base alla quale il traffico dei suoi cittadini deve rimanere all'interno del Paese ed essere sempre accessibile alle forze di polizia. Sia gli USA sia la Gran Bretagna stanno facendo pressioni sulle aziende dalla Silicon Valley per avere accesso alle comunicazioni cifrate e, dopo gli attacchi di Parigi, anche la Francia sta prendendo in considerazione la possibilità di rendere Tor illegale e chiudere l'accesso al WiFi pubblico. A prescindere dalle questioni politiche, è chiaro che i governi di tutto il mondo stanno cercando di regolamentare Internet e ciò avrà un enorme impatto sulla sicurezza delle singole attività e dell'intero Internet. Se non dedicheremo abbastanza attenzione alla trasformazione di questo scenario, le nuove leggi ci coglieranno alla sprovvista: una condizione in cui un professionista della sicurezza non vorrebbe mai trovarsi.
- **Lo sconosciuto inconoscibile**
  Se alcuni fatti possono essere previsti, altri sono totalmente fuori da ogni previsione. Posso dire con tranquillità che ogni organizzazione subirà nel 2016 almeno un incidente che non poteva essere previsto sulla base delle proiezioni nel futuro dei trend attuali. Il segreto dei professionisti della sicurezza è quello di saper identificare il maggior numero possibile di minacce conoscibili e quindi saper costruire un programma di difesa abbastanza flessibile da potersi adattare anche alle minacce sconosciute. Avete un piano per la ricostruzione dei vostri server web nell'eventualità di una compromissione? Cosa succede se vengono colpiti i vostri server AD? Consideriamo il peggiore degli scenari: abbiamo un piano per il caso in cui l'intera rete cada sotto il controllo di qualcun altro? Sembra un'esagerazione, ma è ciò che è successo, ad esempio, a Sony e OPM negli USA e probabilmente a molte altre organizzazioni che sono riuscite a non fare trapelare la notizia. Analizzate tutti i vostri processi e procedure assicurandovi che siano in linea con il vostro obiettivo di mantenere l'azienda al sicuro, anche se dovesse accadere qualcosa di totalmente imprevedibile. Qual è il vostro piano per l'invasione degli zombie? Probabilmente non sarà molto diverso dal piano per un'epidemia contagiosa.

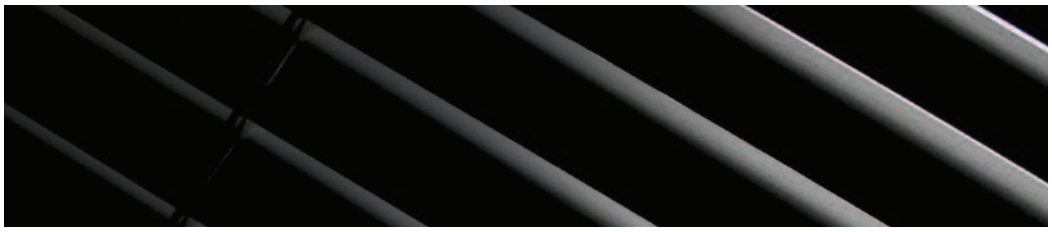
Sebbene nessuno abbia la sfera di cristallo per prevedere con certezza gli accadimenti del futuro, è fondamentale che le aziende mettano in campo strategie che riescano a mitigare il più possibile gli effetti collaterali di un attacco. ■

6 trend che gli MSP dovrebbero cogliere al volo!

Gli MSP devono essere al passo con i nuovi trend del settore e l'evoluzione delle nuove tecnologie. Questo è essenziale per garantire loro di essere sempre un supporto di qualità per i clienti e per assicurare un'attività redditizia. Spesso la sfida è trovare il giusto equilibrio tra la gestione dell'attività in un contesto in continuo cambiamento, mantenendo il controllo su tutti gli asset. Ciò significa che, oltre a standardizzare e ottimizzare le configurazioni e i processi attuali, gli MSP devono essere al corrente delle nuove tecnologie, restando però flessibili, e capire quando ha senso andare avanti, apportando dei cambiamenti al proprio portfolio, oppure attraverso investimenti.

Esistono diversi trend che possono avere un impatto sui clienti attuali e gli MSP dovrebbero conoscerli per garantire la migliore assistenza possibile e per essere all'altezza delle aspettative dei clienti. Di seguito, i sei trend principali che gli MSP dovrebbero cogliere al volo, per non essere superati dalla concorrenza:

1. **Windows 10** – Windows 10 è un ottimo sistema operativo, ma gli MSP devono ancora tutelare e mettere in sicurezza i dati del cliente all'interno di questo sistema. A parte alcune difficoltà tecniche iniziali e alcune questioni di sicurezza, Windows 10 ha mostrato miglioramenti reali, introducendo caratteristiche come la firma unica e l'autenticazione a due fattori. Gli MSP dovrebbero assicurarsi che i clienti siano consapevoli di ciò che comporta per il successo della propria organizzazione l'aggiornamento a Windows 10. Inoltre, dovrebbero essere preparati a rispondere a domande riguardo alcuni aspetti di sicurezza, compatibilità e implementazione per garantire ai clienti una transizione senza problemi. Infine, i clienti degli MSP faranno riferimento a loro per comprendere fino in fondo il valore aggiunto apportato da Windows 10, e una buona riuscita per gli MSP dipenderà dalla loro capacità di articolare queste informazioni secondo il contesto di ogni cliente.
2. **Machine Learning** – Il machine learning ha il potenziale per cambiare radicalmente il modo in cui gli MSP offrono i propri servizi ai loro clienti. Al momento, il machine learning rappresenta un territorio relativamente inesplorato per gli MSP, e i fornitori di piattaforme di gestione dei sevizi di IT Cloud che hanno accesso a community intelligence hanno la chiave per dare un vero valore aggiunto ai dati. Sfruttando appieno gli insight delle community, i fornitori di servizi IT possono accedere a insight basati sui dati in tempo reale, con notizie estrapolate da varie fonti, raccolti attraverso i dispositivi gestiti dagli MSP che utilizzano quella piattaforma di gestione IT. Gli MSP dovrebbero capire e fare in modo che i benefici offerti dal machine learning siano una priorità nel prossimo anno, dato che questo li aiuterà a migliorare decisamente i propri servizi e accrescere il valore aggiunto che apportano, senza grandi investimenti o tempi biblici.
3. **Internet of Things** – IDC, un'azienda di ricerche di mercato, auspica che il mercato globale dei dispositivi e dei servizi legati all'Internet of Things supererà i 7 mila miliardi di dollari entro il 2020. Seppure impressionanti, questi dati portano molte aziende a domandarsi



che cosa fare con la propria strategia IoT. Gli MSP dovrebbero proporre l'IoT nel proprio portfolio come un'opportunità in più, ma con tutto il clamore che oggi c'è intorno a questo mercato, è difficile capire quali aspetti siano realistici e attuabili. Gli MSP dovrebbero ritagliarsi del tempo per analizzare i vantaggi e gli svantaggi dell'IoT prima che questo arrivi al massimo del proprio potenziale. Con così tante tecnologie nuove, le aziende non hanno il tempo necessario per prepararsi prima dell'applicazione. È importante iniziare adesso l'iter di formazione per sviluppare la strategia più indicata e l'impostazione giusta per lo sviluppo. Invece di applicare una tecnologia e informarsi a proposito in corso d'opera, le aziende hanno la possibilità di aggiornarsi adesso e trarre tutti i vantaggi possibili dall'IoT.

4. **Il mobile in azienda** – Secondo il Mobile Analytics Report, il totale dei dispositivi mobili aziendali a livello mondiale l'anno scorso è aumentato del 72%. Gli MSP devono padroneggiare l'applicazione dei servizi cloud e la gestione dei dispositivi mobili aziendali, per poter così gestire la percentuale sempre più elevata di dipendenti che lavorano al di fuori dei propri uffici. Fornire semplicemente i dispositivi non basta! Gli MSP devono applicare le soluzioni mobili in azienda, per disporre anche degli strumenti più indicati alla gestione di questi dispositivi da remoto.
5. **Un IT più consumer** – Sempre più spesso chi lavora porta sul proprio posto di lavoro tecnologie e dispositivi "consumer market", e questo sta cambiando il modo in cui i dipendenti e le aziende concepiscono le informazioni. Secondo uno **studio di IDG**, la proliferazione di dispositivi personali usati a scopo lavorativo ha portato l'82% delle organizzazioni ad attuare cambiamenti, come l'introduzione di politiche sulla condivisione dei dati aziendali, e ad acquistare soluzioni per far fronte a queste sfide. I clienti faranno riferimento agli MSP per una soluzione che dia una visibilità completa a tutti i livelli del network e soddisfi i criteri di sicurezza.
6. **CIO virtuale / consigliere fidato** – Spesso le organizzazioni necessitano di una guida per orientare le loro attività nella direzione giusta riguardo la strategia IT e le operazioni in quest'ambito. Invece di assumere un membro dello staff IT in sede, sempre più organizzazioni, se necessitano di know-how IT on demand, si rivolgono a un CIO virtuale. Poter contare su un partner di fiducia per l'IT è estremamente utile nel superare il gap di tecnologia delle organizzazioni, e allineare strategicamente la tecnologia agli obiettivi di business. Gli MSP dovrebbero sempre concentrarsi esattamente su ciò che l'azienda cliente chiede, dato che c'è sempre una discrepanza tra ciò che i dipartimenti IT vogliono acquistare e ciò che i fornitori di servizi IT cercano con tutte le proprie forze di vendere. Una **ricerca** evidenzia che il 71% dei fornitori di servizi IT vuole un rapporto con i propri clienti più strategico, ma solo il 13% dei dipartimenti IT pensa lo stesso. Diventare un CIO virtuale di fiducia è più di una condivisione di know how tecnico, significa allineare la visione degli MSP per offrire ai dipartimenti IT proprio ciò di cui hanno bisogno. ■

Cyber Intelligence: un passo avanti alle minacce

Le minacce informatiche stanno diventando sempre più parte integrante del tessuto digitale aziendale e gli attacchi mirati diventano sempre più subdoli e dinamici. Questa evoluzione nelle metodologie di attacco ha fatto emergere i limiti degli approcci tradizionali di sicurezza. Chi subisce un attacco deve potenziare le proprie capacità nell'individuare e riconoscere le minacce nei propri sistemi aziendali per ritornare ad essere in vantaggio sull'attaccante e agire per tempo in modo preciso ed efficace. La Cyber Intelligence è fondamentale per questa sfida in quanto fornisce una visione totale, personalizzata e in tempo reale delle anomalie emergenti – contrariamente al precedente approccio basato su firme e regole che diventano obsolete dato che si riferiscono a minacce già individuate. L'approccio basato sull'Intelligence è il cuore della Cyber Defense di nuova generazione; vengono impiegati personale qualificato e tecnologie all'avanguardia di tipo 'sistema immunitario' in un processo costante di apprendimento e comprensione delle problematiche in evoluzione per poterle contrastare prima che diventino critiche.

RESTARE APERTI PER LAVORARE

Oggi la violazione del perimetro della rete aziendale viene considerata inevitabile dagli operatori di sicurezza. Questa è la nuova realtà: le tecnologie operanti sul perimetro aziendale pur ricoprendo un ruolo cruciale in un sistema stratificato di difesa, sono insufficienti per sconfiggere un attacco mirato. È ormai accettato che le violazioni siano inevitabili e il loro verificarsi sia più un discorso di 'quando' che di 'se'. In questo nuovo mondo la sfida è cambiata. Oltre a difendere il proprio perimetro aziendale si devono affrontare anche le minacce interne utilizzando un approccio basato sull'Intelligence per indirizzare pericoli reali all'interno di una rete complessa.

Le aziende moderne devono essere in grado di operare in un mercato aperto e connesso. La linfa vitale di un'azienda sono i dati e per crescere un'azienda ha bisogno che questi possano circolare sia fuori che dentro i tradizionali perimetri di rete. I dati vengono scambiati costantemente fra l'azienda e i suoi clienti, i fornitori, il personale, i soci e così via. La sfida del CISO oggi è quella di proteggere i suoi dati che sono alla mercé di chiunque. In effetti tutti i progressi tecnologici che hanno consentito alle aziende di prosperare negli ultimi dieci anni - la connettività, la digitalizzazione, l'innovazione - sono quelli che le espongono ai rischi maggiori. Chi opera nella sicurezza oggi sa come gestire i comportamenti del personale di un'azienda. Pur considerando i lavoratori come risorse di valore e meritevoli di fiducia, questi rappresentano una minaccia significativa per l'integrità dei dati aziendali e il loro comportamento, doloso o colposo, aumenta il rischio per l'azienda. Anche se c'è la tentazione di aumentare i controlli e introdurre norme operative più stringenti la necessità di lavorare fa sì che le persone trovino il modo di aggirarle. Chiunque vi dirà che è possibile curare qualsiasi malattia ammazzando il paziente. Un'azienda non può essere soffocata da controlli di sicurezza laboriosi e poco pratici pensando di rimanere più sicura a spese dell'efficienza, dell'agilità e della competitività. Oggi la sfida per gli operatori della sicurezza consiste nel difendere il patrimonio aziendale più prezioso, i dati, consentendo a essi di facilitare la crescita.

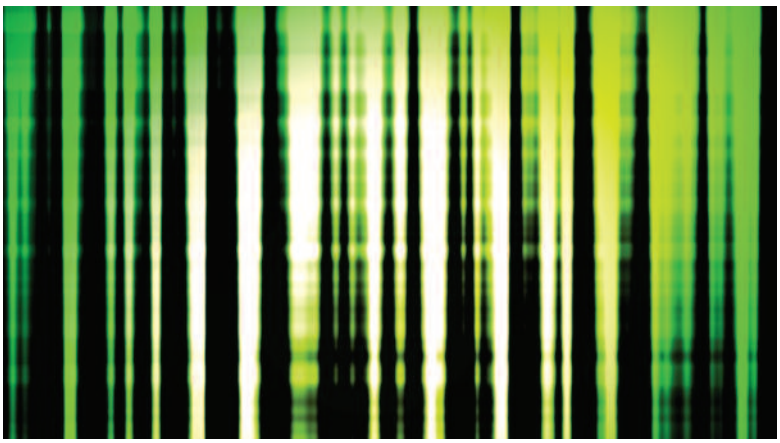
In questo scenario dove le minacce sono in continua evoluzione continuare a lavorare ri-

chiede un equilibrio fra i rischi e i benefici. L'equilibrio necessario non è mai totalmente statico, ma viene riadattato continuamente per mantenere uguali i pesi sui due piatti della bilancia. Questa sfida richiede un approccio sottile, orientato all'Intelligence più che alla sicurezza. Mentre la sicurezza informatica presuppone che le misure di difesa debbano funzionare il 100% delle volte, la Cyber Intelligence fornisce suggerimenti, basati su prove, che indirizzano il processo decisionale, fa emergere le problematiche di alto livello rispetto a quelle meno importanti e consente alle aziende un miglior controllo e una migliore consapevolezza sul proprio stato di salute per poter definire la migliore strategia per la cura.

PASSARE SOTTO AI RADAR

Ogni settimana le notizie di attacchi informatici vengono riportate sulle prime pagine dei giornali con riferimento a numeri vertiginosi di conti compromessi e impatti reputazionali non indifferenti.
Le intrusioni più eclatanti richiedono azioni di risoluzione immediate con impiego di risorse economiche, temporali e umane per ripristinare ciò che è stato compromesso.
Il concetto di operazione di ripristino a seguito di un attacco informatico è però incompleto. Le aziende non sono mai completamente esenti da minacce o da elementi potenzialmente pericolosi o malevoli. C'è una forte pressione affinché le aziende corrano ai ripari dopo un attacco per mitigare il danno d'immagine e per recuperare la credibilità nei confronti dei clienti e degli azionisti; questo però è classificato come 'troppo poco e troppo tardi'. Troppo tardi perché il danno è stato fatto, troppo poco perché l'avversario è riuscito comunque a controllare e infiltrarsi nell'azienda evidenziandone a posteriori la limitata capacità di difesa.
La sfida degli ultimi anni si è acuita a causa dell'industrializzazione dell'economia che ruota intorno ai crimini informatici e alla sempre più raffinata abilità degli esecutori. Su internet si trovano avanzati strumenti di attacco pronti all'uso – è possibile provare, scambiare e vendere nuove forme di attacco

e malware configurabili – e questo a riprova di come sia banale infiltrarsi in un'azienda. Una volta infiltratisi, gli attacchi hanno luogo in forma anonima rendendoli difficili da individuare perché in incognito e effettuati con cautela.
Per prima cosa, dall'esterno, l'aggressore userà le credenziali di accesso di un dipendente per non far scattare gli allarmi ubicati sul perimetro. Questo approccio rende estremamente difficile distinguere fra un'attività lecita e quella di un malintenzionato intento a fare danni. Gli aggressori utilizzano questo velo di legittimità per portare a termine i loro attacchi mimetizzandosi fra le normali azioni di quell'utente nel corso delle sue attività quotidiane sulla rete. Essere riconosciuti come utenti regolari offre un vantaggio agli aggressori. Essendo considerati 'fidati' il compito di muoversi nella rete aziendale ed estrarne dati o manipolarne i sistemi diventa più facile.
Per di più gli aggressori non usano solo campagne di email mirate e sfruttano credenziali legittime per passare sotto ai radar, ma possono anche sfruttare gli zero-day e i malware appositamente sviluppati per raggiungere i propri obiettivi. Sempre di più vengono perpetrati attacchi, portati avanti astutamente e ben mimetizzati, per lunghi periodi di tempo a riprova della pazienza e perseveranza dell'aggressore.
Un attacco di tipo avanzato può restare nascosto nella rete per giorni, settimane o mesi di fila rimanendo pazientemente inattivo nella rete aziendale in modo da renderne l'indi-



viduazione più difficile. Mediamente il tempo necessario a individuare un attacco informatico si aggira sui 170 giorni. Se perpetrato anche con aggressori dall'interno questo valore arriva a 259 giorni.
Durante questo lasso di tempo l'aggressore si fa un'idea dell'architettura della rete e stabilisce come muoversi su di essa per portare a termine l'attacco mirato. Mentre chi si deve difendere è costantemente distratto dalla gestione delle attività giornaliere, l'aggressore ha dalla sua parte il tempo e le risorse con cui effettuare ricognizioni sui sistemi, portare a termine le sue azioni e muoversi evitando di essere scoperto, con relativa tranquillità.
Solitamente un aggressore evoluto cerca di rimanere nascosto a lungo dentro un computer o la rete. Per porsi al riparo da eventuali intercettazioni l'aggressore cercherà di compromettere più dispositivi e server presenti sulla rete. Chi attacca è spesso capace di muoversi su una rete per capire quali siano gli strumenti usati per intercettarlo; questo gli permette di muoversi in modo sufficientemente invisibile per evitare di essere scoperto dai tipici sistemi che basano il loro funzionamento su un insieme di regole. Il traffico della rete e l'elevato volume di dati inviati a sistemi di 'log-management' rendono spesso impossibile rilevare i movimenti invisibili di un aggressore. Nonostante che nella fase di analisi forensica post-attacco sia evidente la prova dell'infiltrazione, salta anche all'occhio come questa possa essere invisibile nel rumore del traffico della rete.

IL TEMPO È PREZIOSO

Il tempo è una risorsa preziosa che manca spesso a chi viene attaccato. L'aggressore determinato ha tempo in abbondanza, finanziamenti sufficienti e risorse umane per sviluppare attacchi che eludano i vari livelli di sicurezza presenti in un'azienda. Le aziende lottano costantemente per rilevare le fasi iniziali di una infiltrazione, prima che vengano fatti danni quali il furto di dati su grande scala o l'interruzione di un servizio essenziale. Invece le aziende si trovano coinvolte in una lotta contro il tempo per rimuovere e ridurre velocemente i danni finanziari e d'immagine, al contrario dei mesi di preparazione e ricognizione che l'aggressore ha a disposizione prima di sferrare il suo attacco. Fintanto che il vantaggio rimane in mano all'aggressore le aziende attaccate saranno sempre sulla difensiva. Le aziende devono ripensare al modo in cui affrontano gli attacchi informatici e la sicurezza informatica. Tanto per cominciare questo vuol dire non considerare questi concetti come assoluti; la sicurezza informatica totale non è possibile in pratica e gli attacchi non hanno perimetri ben definiti: non hanno un inizio preciso e nemmeno una fine. Ogni attacco inizia con una infiltrazione che a sua volta inizia con un cambiamento impercettibile nel normale ordine delle cose e s'ingrandisce fino a diventare una catena di eventi che messi insieme possono esercitare il controllo di un sistema remoto e metterne in pericolo i contenuti. In un'epoca in cui le minacce sono innumerevoli e in continua evoluzione analizzare i problemi di ieri non garantisce la difesa da quelli di domani. Gli aggressori di oggi utilizzano tecniche e strategie in continua evoluzione per rimanere nascosti a lungo nei vostri sistemi. Il riferimento a ciò che è normale è in continua evoluzione.
Occorre quindi iniziare a considerare il tempo in modo diverso, tentare di cogliere attività sospette nella finestra temporale compresa fra l'infiltrazione iniziale e i primi segnali di anomalia. Invece d'investire in analisi post-mortem su intrusioni e compromissioni passate ci si deve sforzare di trovare i problemi di domani, indirizzando le attenzioni verso attività che si mimetizzano nel rumore delle at-

tività quotidiane di un'organizzazione. All'interno dell'IT aziendale ci sono due fattori da tener presente:

Visibilità e comprensione

Le aziende devono fare un passo indietro quando prendono in considerazione le strategie per la difesa informatica, chiedendosi per prima cosa quanto bene conoscano la loro azienda. Le infrastrutture di rete e le intranet sono cresciute e si sono estese aggiungendo sempre più dispositivi, funzionalità e tecnologie; l'architettura digitale di un'azienda di una certa dimensione è solitamente molto complessa.

Gli addetti IT alla sicurezza e dell'architettura spesso non hanno visibilità di tutti i sistemi sotto il loro controllo e si concentrano solo su quelli su cui ci sono problemi noti che richiedono soluzione. La visibilità totale su tutte le interazioni e comunicazioni digitali, non solo su una parte, è critica perché consente agli addetti della sicurezza di prendere le decisioni migliori basandosi sulla conoscenza dell'intero sistema. Avendo visibilità totale sull'andamento e il tipo di traffico gestito giornalmente nell'azienda, gli addetti della sicurezza sono in condizione di configurare al meglio la protezione della rete, identificare le vulnerabilità o i dipendenti infedeli e tenere effettivamente a freno in tempo reale le minacce informatiche. Vedere e capire cosa sta accadendo in tempo reale è il primo passo per conoscere cosa non debba accadere, indipendentemente da quanto sia minimo lo scostamento dalla normalità.

Analisi intelligente e rilevamento anomalie

Avendo la conoscenza delle attività aziendali è possibile usare nuove tecnologie per analizzarle ed avere una chiara visione di quale sia la normalità. I fondamentali progressi nella matematica probabilistica e nell'ambito del 'machine learning' hanno reso possibile questo approccio, usando una tecnologia che impara su base continua ciò che è normale e anomalo nell'ambito aziendale ed evidenzia anomalie su base probabilistica in tempo reale. Le anomalie o le deviazioni da ciò che è stato identificato come normale sui sistemi, le reti e gli utenti devono essere autentiche e basate sulla comprensione dinamica dell'ambiente circostante. Un comportamento difforme spesso può essere affrontato in modo appropriato, ma solo se rilevato nelle sue fasi iniziali. Le aziende devono abbandonare l'approccio che consiste nel dover passare al setaccio l'enorme quantità di allarmi generati da sistemi basati su regole preconfigurate per identificare le minacce e orientarsi verso sistemi d'intelligence, fatti su misura, che aiutano a conoscere l'ambiente digitale aziendale così com'è per prendere le corrette decisioni. Concludendo, si può dire che per ridurre il rischio occorre un esercizio continuo portato avanti da professionisti capaci di prendere le corrette decisioni, la capacità di fare le scelte giuste e di concentrarsi sulle aree d'interesse richiede una nuova generazione di prodotti che sia adattativa, probabilistica e in grado di auto apprendere.

MIGLIORARE LA CONCENTRAZIONE, PER UN'AZIONE MIGLIORE

È quasi impossibile predire le metodologie e le tecniche di attacco; gli attacchi di ieri sono diversi da quelli di domani o dopodomani. Le vulnerabilità interne sono fonte di problemi che richiedono una valutazione continua. In questo contesto, dove innumerevoli minacce sono presenti in qualsiasi momento all'interno di un'azienda, è richiesta una visione completa degli eventi per capire dove concentrare l'attenzione e stabilire in tempo reale le priorità per la Cyber Defense. Di contro, il sovraccarico degli allarmi che vengono generati costantemente dalla pletora di prodotti convenzionali per la sicurezza ottiene come risultato l'abbassamento del livello di guardia da parte del personale addetto alla sicurezza o dell'IT, causato da questo elevato numero di anomalie proposte o dalla inutile natura delle informazioni ricevute.

Gli addetti della sicurezza devono essere in grado di affinare la conoscenza delle minacce in modo che abbiano senso in un contesto aziendale invece di perdere tempo ad analizzare migliaia di allarmi fuori contesto. Avvalersi delle configurazioni proprie di ogni azienda - l'orario in cui i dipendenti arrivano al lavoro, i tipi di dispositivi che utilizzano e

come, le risorse a cui hanno accesso ecc. - è fondamentale poiché nessun attaccante conosce questi dettagli quando pianifica un attacco. Questo livello di granularità deve essere sfruttato utilizzando tecnologie di tipo 'sistema immunitario' che siano 'self-learning' e che possano vedere e analizzare scientemente questi dati, capendone in maniera implicita il livello di normalità o meno e facendo emergere in tempo reale le anomalie che devono essere gestite in modo tempestivo.

'CYBER INTELLIGENCE' CONTRO 'THREAT INTELLIGENCE'

Il termine 'Threat Intelligence' viene usato per la raccolta e la condivisione di informazioni su minacce note. In altre parole si fa riferimento ad un database o insieme di dati da confrontare con gli allarmi di sicurezza rilevati in un'azienda, i log e altri dati forensici per capire se quanto rilevato è una minaccia oppure no. Se quanto rilevato è riconducibile alle informazioni contenute nella 'Threat intelligence' ciò può essere usato per proteggere l'azienda da attacchi simili ancora in circolazione. Il difetto principale nel condividere informazioni riconducibili ad attacchi già avvenuti è che questo approccio 'a posteriori' non aiuta le aziende a difendersi dai nuovi attacchi di domani. Affinché questo funzioni è necessario che almeno un'azienda venga violata da ogni nuovo attacco per poterlo identificare, limitandosi a segnalare gli attacchi già subiti con la speranza che lo stesso si possa ripresentare.

Solitamente occorrono alcuni mesi prima che una nuova tipologia di attacco venga inclusa nella 'Threat Intelligence'; nel frattempo la vostra azienda è vulnerabile a quegli attacchi che devono ancora essere scoperti e condivisi dalle loro vittime. Nella peggiore delle ipotesi è un flusso di dati inutili che distoglie dall'obiettivo principale dell'azienda che è quello di difendersi dai nuovi attacchi, non da quelli già avvenuti. È di scarso sollievo sapere che la vostra azienda è stata la prima a scoprire, e subire, un nuovo tipo di attacco e la prima ad averla aggiunta alla 'Threat Intelligence' affinché gli altri si possano proteggere. La 'Threat Intelligence' deve essere adattata ad ogni singola azienda per essere utile e ad un certo punto deve essere vagliata da un essere umano per poter prendere le appropriate decisioni nei momenti critici. L'intelligence migliore è quella che aiuta un essere umano nel processo decisionale, che gli dà la miglior sicurezza nel prendere decisioni corrette, appropriate e soprattutto in tempi sufficientemente brevi da evitare l'intrusione su vasta scala, un'interruzione dei servizi o un colpo alla reputazione. Quindi la vera 'Cyber Intelligence' non è quella che identifica le minacce e i metodi di attacco già noti, ma si concentra sulla corretta comprensione di ciò che sta avvenendo in azienda con un livello di granularità tale da far emergere anche le azioni più subdole.

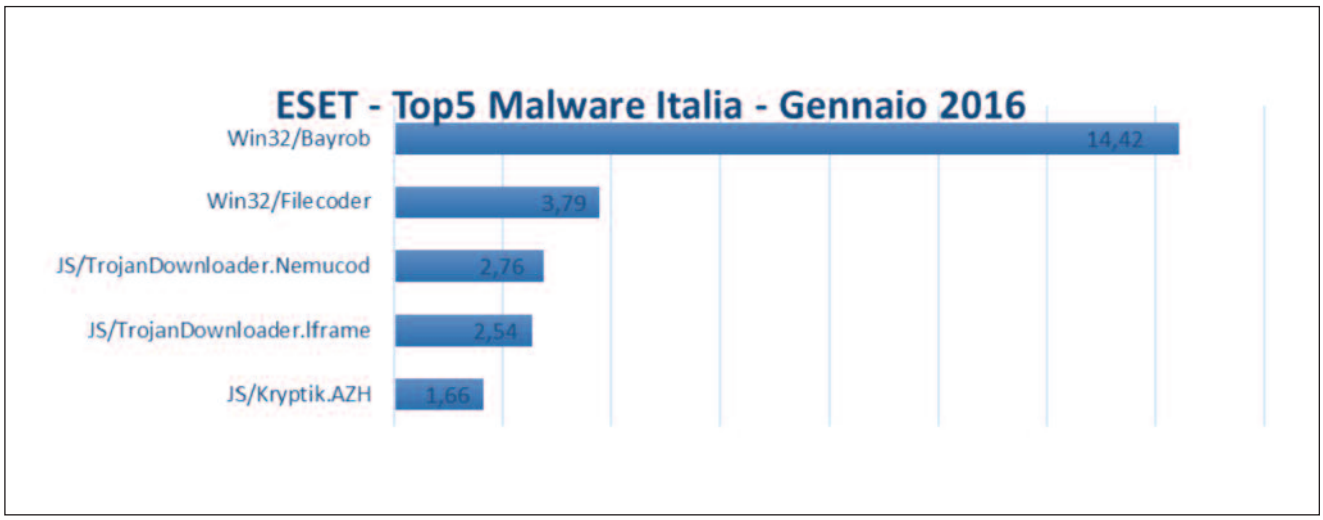
L'intelligence migliore è quella che analizza in tempo reale anomalie ricche d'informazioni e che è in grado di correlare molteplici indicatori deboli per avere un quadro chiaro della situazione. Effettivamente, nell'ambito della sicurezza nazionale e delle forze dell'ordine, il termine 'intelligence' si riferisce ad azioni d'indagine che forniscono informazioni per affrontare rischi e minacce specifiche prima che l'avversario prenda l'iniziativa e vi spinga sulla difensiva. Fornisce una conoscenza, suffragata da prove, che indicano ad un essere umano quando e come passare all'azione e a sua volta confermano l'efficacia delle decisioni su base continuativa dato che il contesto cambia inevitabilmente. Per le aziende che vogliono essere proattive nei riguardi degli attacchi informatici queste domande sono critiche e richiedono azioni d'intelligence di elevata qualità e i riscontri di un'analisi avanzata e sensibile al contesto di un ampio spettro di fattori che contribuiscono all'eventuale attacco. La 'Cyber Intelligence' deve guidare nel prendere decisioni quando le infiltrazioni sono nella loro fase iniziale e gestibile, in una finestra temporale che consenta di verificarne l'efficacia ed evitare che la situazione diventi critica. ■

a cura di Darktrace

La top 5 dei malware in Italia

Il Bollettino ESET di gennaio 2016.
Nome in codice Bayrob: ecco il trojan che a gennaio 2016 ha colpito il 14,42% degli internauti italiani.
Bayrob si nasconde dietro allegati infetti di false email provenienti da Amazon.

Si chiama ***Bayrob e si maschera dietro allegati infetti di false mail provenienti da Amazon***: così questo trojan, conosciuto come minaccia informatica già dal 2007 e rimasto silente per molto tempo, ha registrato da dicembre 2015 un'impennata di infezioni in diversi paesi europei, ***raggiungendo in Italia, secondo le stime dei ricercatori di ESET, la vertiginosa quota del 14,42%.***
Le mail fraudolente che veicolano Bayrob spesso si celano dietro un finto account di Amazon, che però ad un rapido controllo dell'indirizzo di posta del mittente rivelano non avere nulla a che fare con questa società. L'allegato malevolo si presenta come file ZIP contenente un eseguibile che, se scaricato, lancia un ***messaggio ingannevole di "applicazione non compatibile" mentre crea una backdoor*** che verrà utilizzata dai cybercriminali per prendere possesso del PC ormai infetto, rubandone le informazioni sensibili.
Al secondo posto della top5 dei malware di gennaio 2016 sale **Win32/Filecoder**, un temibile ransomware che cripta i file dell'utente e richiede alla vittima un riscatto in cambio del software di decodifica. **Win32/Filecoder** nella prima settimana di gennaio ha registrato in Italia il picco di infezioni a livello mondiale con una percentuale del 6,35.
La Top 5 dei malware in Italia si basa su Live Grid®, l'esclusiva tecnologia Cloud di ESET, che identifica mensilmente le minacce informatiche globali per numero di rilevazioni.



Win32/Bayrob – rilevato nel 14,42 % delle infezioni

Al primo posto della top 5 dei malware di gennaio 2016 sale **Win32/Bayrob**, un trojan che si nasconde dietro email fraudolente contenenti file eseguibili che, una volta lanciati, creano una backdoor dalla quale i cybercriminali tengono in ostaggio il PC infetto, rubandone le informazioni sensibili. Oltre all'Italia, Bayrob ha colpito in Europa la Spagna, con il 22,08% delle infezioni e l'Austria, con il 18,49% delle infezioni.

Win32/Filecoder – rilevato nel 3,79% delle infezioni

Sale al secondo posto nella classifica mensile **Win32/Filecoder**, un trojan che nella prima settimana di gennaio ha registrato in Italia il picco di infezioni a livello mondiale con una percentuale del 6,35%. Win32/Filecoder cripta i file dell'utente e richiede alla vittima un riscatto in cambio del software di decodifica. Per infettare i PC in questo caso gli hacker utilizzano diverse tecniche di infiltrazione come download guidati da siti infetti, allegati email, installazione tramite altri trojan o backdoor, o addirittura installazioni mirate.

Win32/TrojanDownloader.Nemucod – rilevato nel 2,76 % delle infezioni

Scende al terzo posto **Win32/TrojanDownloader.Nemucod**, un trojan che reindirizza il browser a uno specifico URL contenente un software malevolo. Il codice del malware viene di solito inserito all'interno di pagine HTML. Nemucod ha registrato a gennaio 2016 il picco di infezioni in Australia, con una percentuale dell'8,12%, mentre in Europa il paese più colpito è stato il Regno Unito, con il 6,02% delle infezioni.

JS/TrojanDownloader.Iframe – rilevato nel 2,68% delle infezioni

Sale al quarto posto della classifica **JS/Trojandownloader.Iframe**, una serie di trojan che reindirizzano il browser a uno specifico URL contenente un software malevolo. Il codice del malware viene di solito inserito all'interno di pagine HTML.

Questo malware ha registrato il picco di infezioni in Austria con una percentuale del 14,49%, seguita dalla Danimarca, con il 14,09 % e dalla Turchia con il 13,83%.

JS/Kryptik.AZH - rilevato nel 1,66% delle infezioni

Ancora basso nelle percentuali di rilevazione ma in costante ascesa JS/Kryptik, un trojan con un codice malevolo in JavaScript incorporato in pagine HTML. JS / Kryptik di solito reindirizza il browser a un URL dannoso o attua un exploit specifico. ■

a cura di Eset

BOOLEBOX ON-PREMISES

Proteggi i tuoi dati aziendali con BooleBox

BooleBox

Per tutte le realtà che necessitano o preferiscono conservare "in casa" i dati aziendali, BooleBox è la soluzione ideale per integrarsi nell'infrastruttura IT di qualunque azienda.

Ecco perché BooleBox è diverso

Scopri come proteggere, condividere e inviare via e-mail i tuoi dati cifrati tramite BooleBox. In tutta semplicità e sicurezza.

Proteggi i tuoi file con una chiave che conosci solo tu

Utilizza la tua chiave privata per cifrare i tuoi dati. Dai l'accesso ai tuoi file solo a chi desideri.

Secure Mail

Proteggi le tue comunicazioni tramite e-mail che potrete leggere solo tu e il tuo destinatario.

Cifra i tuoi file sia sul dispositivo che durante la sincronizzazione

I file sul tuo PC restano sempre privati e protetti, anche in caso di furto.

Condividi i tuoi file in maniera facile ma soprattutto sicura

Sei tu a controllare le autorizzazioni e gli accessi ai tuoi dati.

www.boolebox.com www.booleserver.com

BOOLE™ server

CYBER CRIME CONFERENCE

LE NUOVE MINACCE DEL CYBER SPAZIO

7° Edizione

12 APRILE 2016
ROMA

HOTEL ROMA AURELIA ANTICA
Via degli Aldobrandeschi, 223

ISCRIZIONI SUL SITO
WWW.TECNAEDITRICE.COM