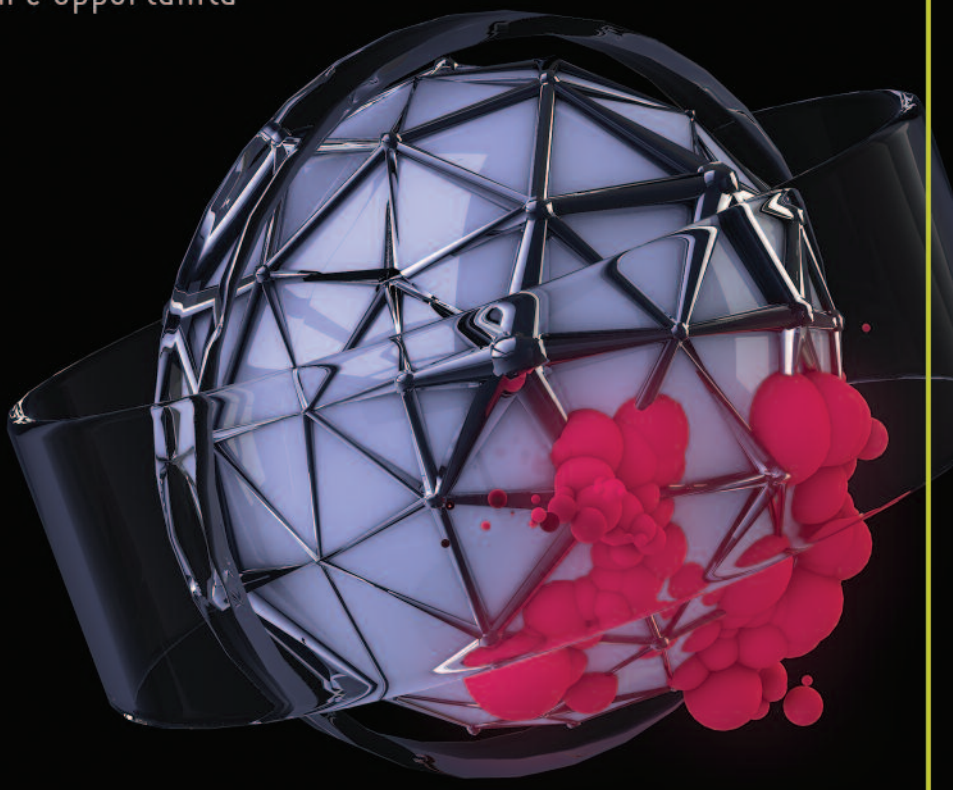
Anno XV
Aprile 2016
Poste Italiane S.p.A.
Spedizione in Abbonamento Postale
D.L. 353/03 (Conv. in L. 27/02/2004 n° 46)
Art. 1, Comma 1 – Roma Aut.n C/RM/44/2012
per "ICT SECURITY" id sap 30619433-015
Prezzo € 9,00

ICT Security MAGAZINE

2016 135

www.ictsecuritymagazine.com

- Cyber Risk Management – problemi e opportunità
- Privacy shield e cloud
- Polizze assicurative cyber
- Nuovo regolamento generale sulla protezione dei dati
- "Cyber strategy & Policy brief"
- Firma elettronica avanzata nel regolamento UE n. 910/2014



TecnaEditrice

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.

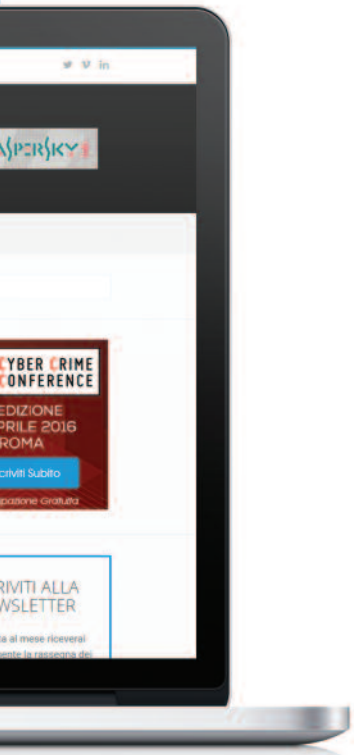
Realizzato per adattarsi automaticamente a tutti i dispositivi di navigazione (pc, tablet, smartphone).

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

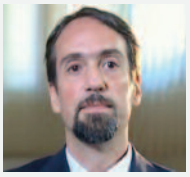
Coordinatore Rubrica
FATTORE UMANO E AMBIENTE DIGITALE

Stefano Mele

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

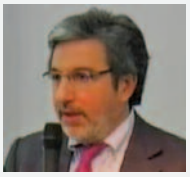
Coordinatore Rubrica
CYBER SPAZIO E SICUREZZA NAZIONALE

Comitato Scientifico



Matteo Cavallini

Responsabile Standard Sicurezza e Sistemi Informativi, Consip



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

Paolo Dal Checco

Consulente Informatico Forense

Coordinatore Rubrica
DIGITAL FORENSICS

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

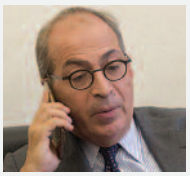
Esperto di dematerializzazione e sicurezza ICT

Coordinatore Rubrica
BIOMETRIA E FIRME ELETTRONICHE

Alberto Manfredi

Presidente CSA (Cloud Security Alliance)

Coordinatore Rubrica
CLOUD SECURITY



Paolo Scotto di Castelbianco

Responsabile delle comunicazioni istituzionali e Direttore della Scuola del DIS

Domenico Vulpiani

Coordinatore dei sistemi informativi, Ministero dell'Interno

Andrea Zapparoli Manzoni

Board Advisor del Centre for Strategic Cyberspace & Security Science di Londra

Coordinatore Rubrica
CYBER RISK

SOMMARIO

COLOPHON

Anno XV - Numero 135 - **Aprile 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 Aprile 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

EDITORIALE

RUBRICHE

ARTICOLI

SELEZIONATO DALLA REDAZIONE

GRANDE SUCCESSO PER LA 7° EDIZIONE DEL CYBER CRIME CONFERENCE 2016

Si è conclusa con grandissimo successo la **7° edizione** della **Cyber Crime Conference** tenutasi lo scorso 12 Aprile presso il Centro Congressi Roma Aurelia Antica.
937 visitatori, suddivisi nelle due aule parallele, hanno assistito attivamente ai contributi di illustri ospiti e personaggi di altissimo prestigio come l'Onorevole **Domenico Rossi**, *Sottosegretario al Ministero della Difesa*, **Rita Forsi**, *Direttore Generale dell'ISCOM del Ministero dello Sviluppo Economico*, **Roberto Di Legami**, *Direttore della Polizia Postale e delle Comunicazioni*, **Silvia Portesi**, *Network and Information Security – Research and Analysis Expert at ENISA*. A moderare i due incontri simultanei: **Barbara Carfagna**, *giornalista di TV7 e Speciale TG1*, e **Patrizia Licata**, *giornalista e collaboratrice di Formiche.net*.
Nelle tavole rotonde si sono affrontate tematiche attualissime e di estremo interesse: "La rete come arma: la convergenza tra terrorismo e cyber-spazio" e "La cooperazione pubblico-privato tra i SOC e le Istituzioni".
L'ISIS rappresenta senza ombra di dubbio la principale minaccia terroristica per tutti i Paesi occidentali. Il numero sempre più elevato di cittadini europei coinvolti in azioni terroristiche ha portato da tempo gli esperti del settore a riflettere in modo più attento e approfondito sui

metodi e i mezzi utilizzati da questa organizzazione terroristica per radicalizzare e plasmare la mente dei futuri martiri. Ciò soprattutto in considerazione della loro distanza dai territori di radicalizzazione delle dottrine religiose e la loro vicinanza per nascita e per cultura ai principi occidentali. In quest'ambito, uno degli strumenti maggiormente utilizzati ed efficaci, è senza dubbio la rete Internet.
La prima tavola rotonda ha approfondito queste tematiche mettendo a fuoco il ruolo che internet e le tecnologie hanno nella strategia dello Stato Islamico al fine di qualificare al meglio questa minaccia per delineare possibili soluzioni di contenimento.
Nella seconda tavola rotonda, con i nostri interlocutori del mondo istituzionale, dell'impresa privata e dei Security Operation Centers (SOC), si sono approfondite le procedure con le quali i SOC collaborano con le istituzioni e il ruolo che questi centri svolgono nel prevenire e combattere il cyber crimine: case studies, best practices e difficoltà in questo compito cruciale di monitoraggio della sicurezza informatica. In modo particolare è stato approfondito il nodo della privacy, molte volte considerata l'antitesi della security.
Hanno dato il loro contributo scientifico (in ordine alfabetico):
Arije Antinori, *CRI.ME LAB "Sapienza" Università di Roma, Dip. di Comunicazione e Ricerca Sociale CORIS*; **Stefano Bargellini**, *Safety, Security, Property and Facilities Director at Vodafone Italia*; **Isabella Corradini**, *Presidente centro ricerche Themis Crime*; **Gerardo Costabile**, *Head of Security & Safety at Fastweb*; **Giuseppe Di Somma**, *Presidente Cifit – Criminology International Forensic Investigation Thechnologies*; **Paolo Dal Checco**, *consulente informatico forense*; **Luisa Franchina**, *Presidente di AIIC*; **Corrado Giustozzi**, *Membro del Permanent Stakeholders' Group di ENISA*; **Carlo Mauceli**, *National Technology Officer di Microsoft*; **Stefano Mele**, *of Counsel di Carnelutti Studio Legale Associato, Avvocato specializzato in Diritto delle Tecnologie, Privacy, Sicurezza delle informazioni e Intelligence*; **Alessio Pennasilico,** *Strategic Security Consultant;* **Gian Luigi Savioli**, *responsabile Security Monitoring & Incident Handling per Telecom Italia;* **Giuseppe Vaciago**, *Avvocato esperto in diritto penale societario e delle nuove tecnologie;* **Valerio Vertua**,*Vice Presidente di CSA Italy e Presidente di Digital Forensics Alumni;* **Stefano Zanero**, *Professore associato, Politecnico di Milano.*
Numerosi anche gli interventi di aziende operanti nel settore, che hanno profilato scenari ed offerto soluzioni su: protezione delle infrastrutture critiche, accessi privilegiati, machine learning, protezione dalle nuove minacce, sicurezza dei droni, evoluzione tecnologico-criminale, hacking back, botnet, cyber risk management, digital forensics, sicurezza nel cloud e molto altro.
Hanno dato il loro contributo (in ordine alfabetico):
Francesco Armando, *Technical Account Manager Qualys Italia;* **Gianni Baroni**, *Amministratore Delegato Gruppo Daman;* **Corrado Broli,** *Country Manager Italy Darktrace;* **Michele Fiorilli**, *Pre-Sales Area Manager DGS*; **Giovanni Giovannelli**, *Senior Sales Engineer Sophos Italia;* **Joseph La Mela**, *Sales Manager Centro Sud Cyberark;* **Valerio Pastore**, *President, Chief Technology Officer e Fondatore di Boole Server;* **Marcello Romeo**, *Presales Manager Italy, Intel Security;* **Marco Zanovello**, *Program Manager Var Group, Security Team Yarix;* **Andrea Zapparoli Manzoni**, *Head of Cyber Security, KPMG Advisory SpA.*
Ricordiamo il Patrocinio dell'**Agenzia per l'Italia Digitale**, del **Ministero dello Sviluppo Economico**, dell'**ISCOM**, di **ENISA**, del **CIS**dell'Università "Sapienza", del **Laboratorio Nazionale di Cyber Security** del **CINI.**
Il Cyber Crime Conference è, ora più che mai, acclamato come l'unico evento in Italia che può offrire una formazione completa e gratuita a tutti i visitatori, sia dal punto di vista teorico che da quello pratico.
Prossimo appuntamento: **17° Forum ICT Security 19 ottobre 2016** – Centro Congressi Roma Aurelia Antica. ■

CYBER RISK MANAGEMENT PROBLEMI E OPPORTUNITÀ

Andrea Zapparoli Manzoni,
Board Advisor del Centre for Strategic Cyberspace & Security Science di Londra

INTRODUZIONE

Oggi la diffusione e la pervasività di reti, infrastrutture, applicazioni, dati e delle loro infinite interfacce con i relativi utilizzatori umani rendono sempre più sfumata la linea di demarcazione tra ambito "fisico" (Geospace) e "virtuale" (Cyberspace), tra l'interno e l'esterno di un'organizzazione, tra fornitore e cliente, tra ambito lavorativo e personale, etc.
In conseguenza di ciò, oltre ad una serie di innegabili vantaggi si determinano anche inevitabilmente nuovi rischi, i quali devono essere individuati in modo puntuale, monitorati strettamente e gestiti opportunamente. L'evoluzione rapidissima delle minacce che si originano nel/dal c.d. "Cyberspazio", inteso come nuovo ambito di operatività per tutti gli stakeholder della nostra società, dai cittadini ai governi alle imprese, sta generando un vero e proprio terremoto nella gestione del rischio, rendendo obsoleti gli strumenti e le metodologie tradizionali.
Questo terremoto si sta estendendo anche alle attività di Governance, Assurance, Compliance e Sicurezza (fisica e logica), tramite le quali oggi si cercano di implementare, con risultati spesso non brillanti, contromisure ai nuovi "rischi Cyber".
Nel giro di pochi anni tutto il settore "Security" nel senso più esteso ne uscirà fortemente trasformato, e chi non potrà o non vorrà anticipare questa fortissima spinta al cambiamento dovrà farsi carico di costi crescenti causati da continui attacchi, destinati a diventare sempre più gravi con il passare dei mesi e degli anni.
Questo principalmente perché gli attaccanti sono usciti dalla fase "artigianale" ed hanno industrializzato le proprie capacità offensive, automatizzandole con grande capacità tecnica ed amplificando così la minaccia "cyber" di ordini di grandezza in breve tempo: alla luce di questo fenomeno e delle sue implicazioni, già oggi ogni organizzazione dovrebbe essersi dotata di un processo di Cyber Risk Management efficace, in base alle proprie esigenze e risorse, pena l'impossibilità di funzionare correttamente e/o sopravvivere nel Cyberspazio.
E' opportuno qui sottolineare che "Cyber Security" non è sinonimo di "Information & Communication Technology Security" dal momento che ormai, a causa dell'applicazione ubiqua delle tecnologie digitali e dell'iper-connessione tra tutti gli elementi (sia in termini di estensione che di complessità), possono essere colpiti da minacce *provenienti* dal Cyber Spazio as-

Andrea Zapparoli Manzoni si occupa con passione di ICT Security dal 1997, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. Fa parte dei Consigli Direttivi di Assintel e di Clusit, è stato membro dell'OSN (Osservatorio per la Sicurezza Nazionale), ed è Board Advisor del Center for Strategic Cyberspace + Security Science di Londra. Presidente de iDialoghi per oltre 10 anni, dal 2014 è Senior Manager della divisione Information Risk Management di KPMG Advisory, con la responsabilità dell'area Cyber Security. E' spesso chiamato come speaker a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. E' co-autore del "Framework Nazionale di Cyber Security". Per il "Rapporto Clusit sulla Sicurezza ICT in Italia" da cinque edizioni cura la sezione relativa all'analisi dei principali attacchi di dominio pubblico a livello globale, ed alle tendenze per il futuro.

set materiali ed immateriali di ogni genere, che nella maggior parte dei casi non sono (solo) Information.
A titolo di esempio un attacco realizzato per vie informatiche ad un "connected vehicle" che abbia come esito il ferimento o la morte del conducente rappresenta un tipico problema di Cyber Security, dove il principale asset da proteggere è la vita umana, mentre l'aspetto di protezione dell'informazione, per quanto presente, rimane in secondo piano (in quanto uno tra i molti elementi in gioco). D'altra parte un caso del genere non può ricadere esclusivamente nell'ambito di attività della Sicurezza fisica o della Safety, dal momento che gli strumenti di mitigazione di un simile rischio sono per lo più di natura logica.

PRESENTAZIONE DELLA RUBRICA DEDICATA AL CYBER RISK MANAGEMENT

A causa di questa continua commistione, già oggi inestricabile, tra fisico e virtuale, nella pratica più ancora che nella teoria l'approccio tradizionale oggi generalmente applicato alla gestione del rischio IT non può fornire gli strumenti utili ad individuare, monitorare e gestire le minacce che si originano nel Cyberspazio.
Questo cambiamento, epocale e rapidissimo, costringe a rivedere con urgenza non solo le metodologie ma soprattutto gli aspetti organizzativi, le prassi, le formule di collaborazione tra diverse competenze e soggetti coinvolti, e sopra ogni cosa, nel breve termine, ci spinge a modificare il *modo di pensare* con riferimento alla gestione di questi nuovi rischi.
Scopo di questa rubrica sarà discutere problemi ed opportunità derivanti dall'esigenza di adottare un processo di Cyber Risk Management adeguato alle circostanze, analizzandone di volta in volta alcuni aspetti salienti.
Anticipando i temi che saranno oggetto dei prossimi articoli della rubrica, per poter impiantare un processo di Cyber Risk Management che sia al contempo sostenibile ed efficace è necessario:

- modificare ed espandere la tassonomia dei rischi per includere i rischi "cyber" nella gestione del rischio tradizionale, al fine di poter disporre di una definizione condivisa e di una adeguata classificazione delle nuove minacce e delle loro possibili conseguenze;
- interpretare i framework, gli standard, le best practices, le normative ed i contratti in modo che riflettano questa nuova tassonomia e siano in grado di renderla "actionable", ovvero utile, in quanto applicabile dal punto di vista operativo. Un buon primo passo in questo senso è il recente "Framework Nazionale di Cyber Security" presentato a Roma lo scorso 4 febbraio, al quale abbiamo avuto l'onore di contribuire tra l'altro proprio la sezione dedicata al Cyber Risk Management, utile per definire i rischi cyber e le relative contromisure ma non sufficiente per poterli gestire;
- definire un proprio Cyber Threat Model (modello di rischio) per poterlo confron-

tare con le informazioni sulle minacce provenienti dall'esterno (cfr punto successivo) ed aggiornarlo continuamente di conseguenza;
- dotarsi della capacità, per nulla scontata o facile da acquisire, di poter misurare in tempo reale la natura, la frequenza e la pericolosità delle nuove minacce emergenti nel/dal Cyberspazio, in modo da poter aggiornare istantaneamente la propria Situational Awareness (alcuni chiamano questo macro-processo "Cyber Intelligence", dando luogo a qualche malinteso tra i non addetti ai lavori), al fine di derivarne una valutazione puntuale del rischio corrente rispetto alla propria realtà specifica (considerato che le minacce "cyber" evolvono con estrema velocità). All'interno di questa componente rientrano anche le attività di Information Sharing, sia in orizzontale (tra "peers") che in verticale (p.es. con gli organi Istituzioni, primo tra tutti il CERT Nazionale);
- elaborare ed arricchire queste informazioni in merito all'evoluzione delle minacce rispetto al proprio Threat Model con un raffronto puntuale rispetto a quanto accade all'interno della propria organizzazione (monitorando e misurando continuamente i fenomeni interni sia dal punto di vista infrastrutturale che applicativo che dei processi di business). Ciò deve avvenire in una logica multidisciplinare dal punto di vista delle competenze coinvolte, e trasversale dal punto di vista dell'organizzazione, ricordando che rispetto alla gestione dei rischi "Cyber" la suddivisione a "silos" delle strutture interne è fortemente penalizzante: non si tratta, lo ripetiamo, di problemi risolvibili autonomamente e compiutamente dall'IT o dall'IT Security senza la collaborazione del Business, delle Risorse Umane, del Marketing, del Legale etc;
- infine, dopo aver fatto tutto il necessario per comprendere la propria superficie di attacco al fine di prevenire ed anticipare le minacce "Cyber", dotarsi dei processi utili alla gestione proattiva, rapida e risolutiva degli incidenti che comunque si verificheranno, facendo in modo che gli esiti di tali analisi non rimangano circoscritti agli ambiti tecnici, ma che le "lezioni apprese" contribuiscano ad aggiornare il Cyber Threat Model e soprattutto vengano rappresentate ad alto livello, ai decisori, di modo che possano disporre di dati reali, dal "campo", per definire a ragion veduta budget e strategie correttive.

Nel prossimo articolo tratteremo di Cyber Threats e della loro tassonomia, e di come impostare un processo di Cyber Risk Management dal punto di vista organizzativo, tecnologico e delle competenze necessarie. ■

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

PRIVACY SHIELD E CLOUD

Valerio Vertua,
Vice Presidente di CSA Italy e Presidente di Digital Forensics Alumni

Il Cloud computing e il trasferimento dei dati verso gli USA sono, di fatto, un binomio molto stretto; nell'attuale assetto di mercato è vero, infatti, che la maggior parte dei servizi Cloud si fondano su server collocati, appunto, negli Stati Uniti o che, comunque, molti fornitori di servizi Cloud abbiano lì la loro sede.
In tale ottica assume quindi una grande importanza l'accordo EU-USA Privacy Schield (di seguito solo "Privacy Schield") che dovrebbe assicurare ai cittadini dell'Unione Europea un trattamento dei dati da parte delle aziende americane in conformità con la normativa europea per la tutela del trattamento dei dati (c.d. normativa privacy).
Prima però di entrare nel merito di questo provvedimento è bene ripercorrere, seppure in maniera sintetica, gli antefatti che hanno determinato il presente quadro giuridico-fattuale. Come noto, il 6 ottobre 2015, la Corte Europea di Giustizia si è pronunciata sulla causa C-362/14 Maximillian Schrems v Data Protection Commissioner con una sentenza dagli effetti dirompenti e che hanno determinato il venir meno del Safe Harbour (ovvero, in maniera molto semplicistica, quell'accorto fra USA e EU in base al quale il trasferimento di dati verso le società americane che aderivano a detto protocollo era lecito).

I punti salienti della sentenza possono essere così sintetizzati:

- in virtù delle normative vigenti negli USA, le società americane, anche se aderenti al Safe Harbour, devono rivelare i dati personali in loro possesso alla Autorità americane preposte alla sicurezza nazionale, se destinatari di specifica richiesta;
- tale incondizionato e generalizzato accesso ai dati è lesivo del contenuto essenziale del diritto fondamentale al rispetto della vita privata e contrasta con i principi sanciti dalla Direttiva europea per la protezione dei dati 95/46/EC e dalla Carta dei diritti fondamentali dell'Unione europea;
- la mancata previsione di qualsiasi facoltà per il singolo di esperire rimedi giuridici diretti ad accedere ai dati personali che lo riguardano o ad ottenerne la rettifica o la cancellazione viola il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, facoltà, questa, che è connaturata all'esistenza di uno Stato di diritto;
- la decisione della Commissione Europea che attesta che le società aderenti al Safe Harbour degli Stati Uniti garantiscono un adeguato livello di protezione dei dati personali trasferiti da paesi UE (Decisione 520/2000/EC) è invalida in considerazione del fatto che priva le autorità na-

Valerio Vertua: Avvocato Cassazionista con studio in Milano; i settori di attività professionale prevalenti sono: il diritto tributario, il diritto societario e il diritto dell'informatica e delle nuove tecnologie; è perfezionato in Diritto Societario ed in Computer Forensics ed Investigazioni Digitali presso l'Università degli Studi di Milano; è componente della Commissione Giustizia Tributaria dell'Ordine degli Avvocati di Milano; è collaboratore della Cattedra di Informatica Giuridica ed Informatica Giuridica Avanzata della Facoltà di Giurisprudenza presso l'Università degli Studi di Milano; è Presidente dell'associazione DFA (Digital Forensics Alumni); è co-fondatore e Vice-Presidente dell'associazione CSA Italy (Cloud Security Alliance Italy).

zionali di controllo dei loro poteri nel caso in cui una persona contesti la compatibilità della decisione con la tutela della vita privata, delle libertà e dei diritti fondamentali delle persone: la Commissione non aveva la competenza per limitare in tale modo i poteri delle autorità nazionali di controllo;
- spetta quindi alle Autorità nazionali UE per la privacy procedere con le loro valutazioni e determinazioni e decidere l'adeguatezza o meno del livello di protezione dati offerto da un Paese Terzo alla luce sia della Direttiva europea per la protezione dei dati 95/46/EC, sia della Carta dei diritti fondamentali dell'Unione europea.

A valle di questa sentenza, il nostro Garante per la protezione dei dati ha emesso il Provvedimento n. 564 del 22 ottobre 2015 intitolato *Trasferimento dati personali verso gli USA: caducazione provvedimento del Garante del 10.10.2001 di riconoscimento dell'accordo sul c.d. "Safe Harbor"* (Pubblicato sulla Gazzetta Ufficiale n. 271 del 20 novembre 2015), vietando così il trasferimento dei dati personali basato su tale delibera e sui relativi presupposti dal territorio dello Stato verso gli Stati Uniti d'America. Rimaneva, quindi, lecito il trasferimento dei dati personali verso gli Usa se basato sull'adozione di clausole contrattuali standard approvate dalla Commissione Europea o in forza delle Binding Corporate Rules (BCR) oltre, ovviamente alle altre ipotesi contemplate dall'art. 43 codice privacy (ad es. il consenso dell'interessato); così come persisteva la possibilità per ogni singola organizzazione o per ciascun professionista di richiedere al Garante, ex art. 44 codice privacy, una specifica autorizzazione all'esportazione dei dati verso un determinato soggetto USA (in linea teorica l'eventuale risposta autorizzativa dovrebbe intervenire entro 45 gg. come previsto dalla tabella B del Regolamento n. 2/2007 del 14 dicembre 2007 del Garante).

In questo improvviso quadro di incertezza per gli operatori europei, interveniva in data 16 ottobre 2015 il WP29 (come noto l'Article 29 Working Party o Gruppo di Lavoro ex Articolo 29 è l'organismo che riunisce i rappresentanti delle Autorità Garanti per il trattamento dei dati di ciascun Paese europeo) che indicava la fine del mese di gennaio 2016 quale termine per permettere di trovare un'adeguata soluzione con le autorità americane. Detto termine, come prevedibile, non veniva però rispettato.

Il 2 febbraio 2016 si giunge alla definizione di un bozza di accordo, denominato EU-USA Privacy Shield, volto a consentire i trasferimenti di dati personali dall'Unione Europea agli Stati Uniti. Questo accordo quadro è composto da una serie di documenti fra cui:
- i Principi del Privacy Shield;
- l'Allegato 1 redatto dall'International Trade Administration (ITA) del Dipartimento del Commercio americano che regola il programma e descrive gli adempimenti per rendere effettivamente operativo il Privacy Shield;
- l'Allegato 2 relativo agli impegni del Dipartimento del Commercio americano in merito al modello arbitrale previsto dal Privacy Shield;
- una lettera della Commissione Federale del Commercio (FTC) che descrive come darà esecuzione al Privacy Shield;
- una lettera del Dipartimento dei Trasporti che descrive come darà esecuzione al Privacy Shield;
- una lettera dell'Ufficio del Direttore dell'Intelligence nazionale (ODNI) riguardante le garanzie e le limitazioni applicabili alle Autorità di sicurezza nazionale americane;
- una lettera del Dipartimento di Stato americano con un memorandum che descrive il suo impegno ad instituire un nuovo Privacy Shield Ombudsperson per le richieste riguardanti l'ingente attività di intelligence americana;
- una lettera del Dipartimento di Giustizia americano concernente le garanzie e i limiti di accesso ai dati da parte del Governo americano per motivi di amministrazione della giustizia e di pubblico interesse.

Ciò premesso è bene ricordare che la Direttiva 95/46/EC prevede la legittimità del trasferimento di dati personali verso Paesi extra-UE quando questi assicurino un adeguato livello di protezione degli stessi ovvero quando il trattamento risulti conforme ai principi ed alla normativa europea; questo giudizio di adeguatezza è

preso con una decisione della Commissione Europea. Lo scopo precipuo dell'EU-USA Privacy Schield è proprio quello di assicurare un adeguato livello di protezione dei dati personali trasferiti, appunto, verso gli Stati Uniti.
I principi cardine sui cui si fonda questo nuovo accordo quadro possono sintetizzarsi nei seguenti punti:

- l'imposizione di precisi obblighi alle società americane che trattano dati personali di cittadini europei nonché una solida applicazione delle regole previste da questo accordo quadro; questo deve quindi essere trasparente e prevedere dei meccanismi efficaci di vigilanza, delle sanzioni per i casi di inadempimento e delle condizioni rigorose per trasferimenti di dati successivi ad altri partner effettuati dalle società che aderiscono a questo accordo quadro;
- la previsione di garanzie chiare e di obblighi di trasparenza per i casi di accesso ai dati da parte del governo americano; questo principio si fonda su una garanzia scritta degli Stati Uniti all'UE in base alla quale gli accessi delle autorità pubbliche governative americane ai dati dei cittadini europei saranno soggetti a precisi limiti, a meccanismi di controllo, al divieto di accesso generalizzato: quindi un accesso solo se necessario e in maniera proporzionata;
- la possibilità per i cittadini europei di ricorrere, in materia di Intelligence nazionale, alla figura di un Ombudsman, inquadrato all'interno del Dipartimento di Stato americano, che deve essere indipendente dai servizi di sicurezza nazionali: l'Ombudsman si occuperà dei reclami e delle richieste di informazioni presentate dai singoli cittadini europei e avrà l'obbligo di informarli sul rispetto delle normative in materia; questi impegni saranno pubblicati nel U.S. Federal Register;
- la previsioni di diverse possibilità di ricorso per garantire l'effettiva protezione dei diritti dei cittadini europei basate sui seguenti punti:
  - i reclami devono essere risolti dalle imprese americane entro 45 giorni;
  - dovrà essere disponibile un meccanismo di composizione stragiudiziale e gratuito delle controversie;
  - ci dovrà essere la possibilità per i cittadini europei di rivolgersi anche alle loro rispettive Autorità Garanti nazionali che collaboreranno con la Commissione Federale per il Commercio per garantire l'esame e la risoluzione dei reclami proposti dai cittadini europei;
  - esisterà, in ultima istanza, la possibilità di ricorrere ad un meccanismo di arbitrato che sfocerà in una decisione esecutiva;
  - le imprese americane potranno impegnarsi a rispettare il parere delle Autorità Garanti europee, facoltà che diventa un obbligo per le imprese che trattano dati inerenti le risorse umane;
- la previsione di un meccanismo di riesame congiunto annuale in grado di monitorare il funzionamento di questo accordo quadro, ivi compresi gli impegni e le garanzie inerenti l'accesso ai dati per finalità di contrasto alla criminalità e di sicurezza nazionale; questo riesame dovrà essere operato dalla Commissione europea e dal Dipartimento del Commercio degli Stati Uniti con l'intervento di esperti dell'intelligence americani e delle Autorità Garanti europee.

Attualmente il Privacy Shield è sottoposto ad una analisi da parte di un Comitato europeo composto dai rappresentanti degli Stati membri e dal WP29 che dovrà esprimere il proprio parere prima della decisione finale. Analogamente le Autorità governative americane dovranno compiere i passi necessari per porre in essere quanto di competenza. In quest'ottica si deve considerare quanto previsto dagli USA con il Judicial Redress Act. Questa norma, firmata dal Presidente Obama il 24 febbraio u.s., dovrebbe attribuire il diritto ai cittadini europei di adire le Corti giurisdizionali americane per l'esercizio dei diritti in materia di privacy in relazione al trasferimento di dati personali verso gli USA; tuttavia occorre anche segnalare che per l'applicazione del Judicial Redress Act è preventivamente necessaria l'esistenza dell'accordo sul trasferimento dei dati e che tale accordo non deve interferire con la sicurezza nazionale.
In questa nuova prospettiva di un Privacy Shield ancora da perfezionarsi, si ritiene interessante proporre, a chiusura di questo scritto, alcuni spunti di riflessione sen-

za però trarre, volutamente, alcuna considerazione:

- la Corte Europea di Giustizia, con la sentenza sopra citata, ha ritenuto che l'accesso indiscriminato ai dati, quindi anche quelli dei cittadini europei che, ad esempio, utilizzavano e utilizzano servizi cloud di provider americani, da parte delle autorità americane violasse la Direttiva 95/46/EC nonché i diritti della Carta dei diritti fondamentali dell'Unione europea;
- nulla viene detto dalla Corte Europea di Giustizia o dalle Autorità Garanti nazionali sull'analogo accesso ai dati dei cittadini europei effettuato senza distinzione e in maniera massiva da parte delle Autorità pubbliche dei singoli paesi europei (come emerso, ad esempio, dal c.d. Datagate a proposito della Gran Bretagna ed il sistema *Tempora*);
- le autorità pubbliche americane ritengono di poter accedere tranquillamente ai dati di server cloud ubicati all'interno dell'Unione Europea quando questi sono di proprietà o sono gestiti da società americane (a tale proposito è interessante notare la battaglia legale che Microsoft sta portando avanti in merito ad un ordine di un Giudice americano di produzione di dati di un cliente salvati su uno dei suoi server posti in Irlanda, sostenendo che il Giudice dovrebbe, per accedere a detti dati, seguire la strada della rogatoria internazionale prevista dai tratti);
- il secondo comma dell'art. 3 della Direttiva 95/46/EC prevede espressamente che Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali "... aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale";
- il nuovo Regolamento UE sulla protezione dei dati personali prevede analoghe disposizioni al considerando n. 14, all'art. 2 comma 2 lettera e) ed all'art. 21.

In conclusione, al momento l'EU-USA Privacy Shield non è stato ancora sottoscritto né dalle Autorità europee, né da quelle americane; sarà quindi interessante vedere nei prossimi mesi lo sviluppo della materia anche in considerazione del fatto che, a breve, dovrebbe entrare in vigore il nuovo Regolamento UE sulla Data Protection e che l'obiettivo della Commissione Europea è quello di rendere effettivo il Privacy Shield per la fine di giugno 2016. ■

LE POLIZZE ASSICURATIVE CYBER: UN TASSELLO DEL COMPLESSO MOSAICO DI RISK MANAGEMENT

Luisa Franchina,
Presidente di AIIC

Alessandro Pastore

Marco Spada

Le conseguenze di un attacco informatico spaziano dal furto di segreti industriali e informazioni riservate, ai danni reputazionali e la conseguente perdita di business, fino a deterioramenti finanziari o sanzioni amministrative. In risposta a questi sinistri il mondo assicurativo ha creato dei prodotti ad hoc.

Le polizze cyber risk sono presenti sul mercato da almeno un decennio ma dalla seconda metà del 2015 hanno avuto una crescita significativa. Si tratta di un prodotto che non ha bisogno di pubblicità, la violazione informatica di grandi società è ciclicamente sulle prime pagine dei giornali. Nel suo ultimo rapporto di ricerca - *A Guide to Cyber Risk: Managing The Impact of Increasing Interconnectivity* - Allianz Global Corporate & Specialty prevede prevede che **i premi delle cyberassicurazioni nei prossimi dieci anni aumenteranno globalmente dagli attuali 2 miliardi di dollari all'anno a più di 20 miliardi, con un tasso di crescita annuale composto superiore il 20%.**[1]

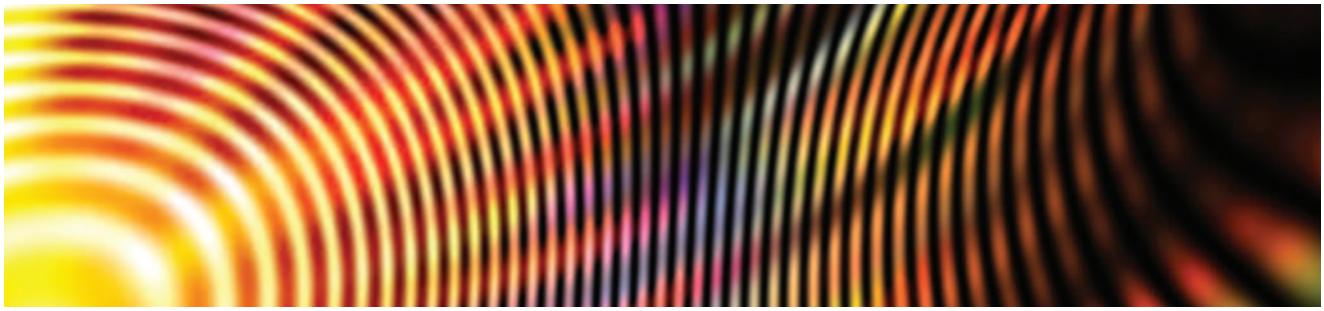
Al momento il mercato è conteso da pochi grandi attori quali American International Group, ACE, Chubb Corp, Zurich

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, gestione dell'informazione e reporting. Docente presso master specialistici di alcune università (Sapienza, Tor Vergata, SIOI - scuola della Farnesina, Campus Biomedico, Bocconi, Università di Milano, ecc.) in temi di sicurezza. Ha pubblicato numerosi articoli e libri su temi di sicurezza e protezione infrastrutture critiche. E' tra gli autori del Framework Nazionale di Cyber Security.

Alessandro Pastore: Analista di intelligence e sicurezza economica. Tra i suoi ambiti di ricerca rientrano la geopolitica degli scenari internazionali, con particolare riferimento alla guerra culturale e all'analisi e la critica dei nuovi media. Nelle sue recenti pubblicazioni si è occupato del rapporto tra social network, radicalizzazione e terrorismo.

Marco Spada: Analista di intelligence per Hermes Bay, dottore in Relazioni Internazionali presso l'Università di Roma Tre con una tesi sul cyberwarfare; attualmente iscritto al Master in Sicurezza delle Informazioni ed Informazione Strategica della Sapienza. Attivo in materia di Analisi su Fonti Aperte, Social Media Intelligence e Cyber Threat Intelligence.

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.



Insurance e pochi altri. Ma l'aumento costante della consapevolezza del rischio e la spinosa questione della privacy, ambito in cui si attende un prossimo intervento normativo anche in Italia, sosterranno una crescita e ramificazione del comparto. Le previsioni sono confermate dal fatto che la fetta di mercato è decisamente ampia e a oggi meno del 10% delle imprese ha una copertura assicurativa di questo tipo. Per le restanti 90%, in caso di attacco informatico, gli amministratori sono i primi ad esporsi a una composita catena di responsabilità, e visto il crescente numero di casi i vertici aziendali non possono ignorare la questione.

Quali procedure devono quindi attivare le aziende per assicurare il loro comparto cyber? **In genere le compagnie assicurative richiedono la compilazione di un questionario inerente la valutazione del rischio che permetta di calcolare il premio assicurativo.** Le società devono fornire un attento esame della postura cyber che evidenzi la quantità di dati sensibili, le policy di protezione di questi, la geolocalizzazione delle sedi, i sistemi di firewall e antivirus, il monitoraggio delle intrusioni, le strategie di backup, le esposizioni sui social network e le strategie di business continuity. **Il fatto che i questionari cambino - anche di molto - da compagnia a compagnia, indica la complessità del prodotto e sottolinea la necessità di una normalizzazione legislativa che tenga il passo delle innovazioni tecnologiche.** Un esempio è rappresentato dai *ransomware*, quei virus informatici che prendono in ostaggio i file attraverso tecniche di crittografia e chiedono un riscatto in denaro: la giurisprudenza italiana non ha ancora prodotto nulla in proposito e in questa eventualità la polizza non garantisce nessuna copertura nel nostro Paese.

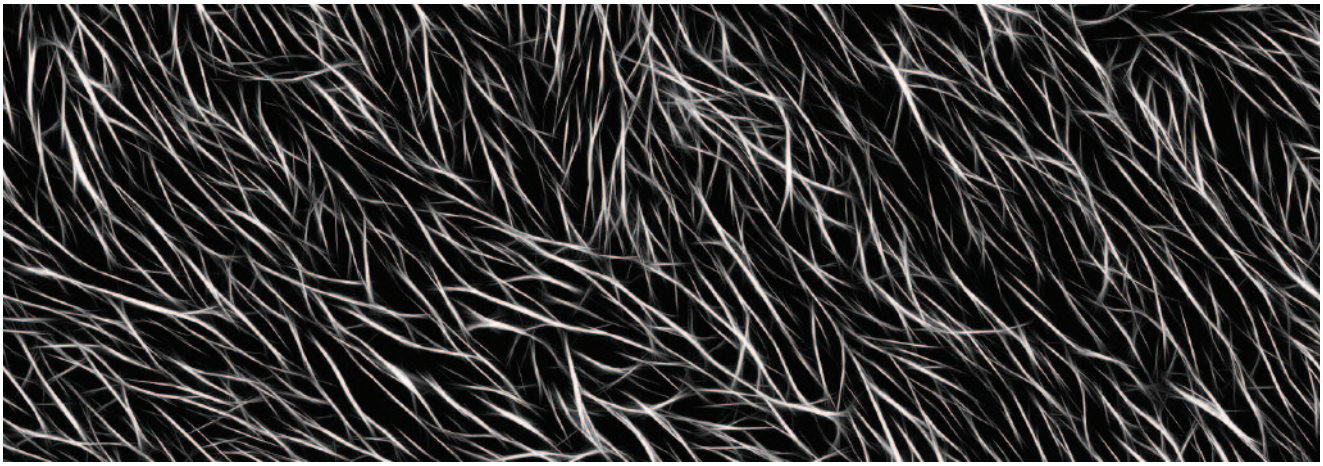
Parlando poi di costi la situazione è ancora in via di definizione e in molti casi le compagnie valutano caso per caso e agiscono in maniera contrattuale. Indicativamente, il costo della polizza varia in funzione del fatturato del cliente e del limite di indennizzo scelto.

Tra le compagnie più attive sul mercato italiano troviamo Allianz AGCS che con la polizza *Cyber Protect* copre i danni provocati da un attacco informatico fino a un massimale di 100 milioni di euro. Generali mette sul mercato *Connected Family*: una polizza domestica, familiare o personale, con uno speciale pacchetto di garanzie legato all'uso di e-commerce, social network e internet in generale. Un altro prodotto ancora è quello proposto da Axa Mps che inserisce la garanzia cyber risk all'interno del pacchetto *Mia protezione* modellato a difesa dell'identità digitale. Quest'ultimo prevede anche una attività di *flooding* che agisce riequilibrando i contenuti dell'utente colpito da danno reputazionale e impedendo alle informazioni negative di comparire nelle prime pagine dei motori di ricerca.[2]

Se all'interno del mondo aziendale il rischio residuo di un possibile attacco in-

1 Allianz Global Corporate & Specialty, (2015), A Guide to Cyber Risk: Managing The Impact of Increasing Interconnectivity, in < http://bit.ly/1YyMUrD > (ultima consultazione 19-03-2016).

2 Per i dettagli delle singole polizze si veda http://bit.ly/1nXqimi; http://bit.ly/1WyhkIf; http://bit.ly/1TWEREK (ultima consultazione 19-03-2016).



formatico può essere trasferito - con qualche riserva come vedremo sotto - alle compagnie assicurative, più complessa è la questione che riguarda il rischio sistemico relativo al contagio e al possibile coinvolgimento delle infrastrutture critiche nazionali. La sempre più diffusa interconnessione al sistema cyber di strutture quali reti idriche ed elettriche aumenta esponenzialmente il pericolo che un attacco informatico localizzato si estenda velocemente con effetti disastrosi per il sistema Paese. Questo è anche il pensiero di Jason Healey della *Cyber Statecraft Initiative for the International Affairs* all'*Atlantic Council* che legge il problema della cyber security in termini di sicurezza nazionale.[3]

La fondatezza di questa prospettiva viene confermata da un recente report del Centre of Risk Studies dell'Università di Cambridge secondo cui un attacco parziale alla rete energetica produrrebbe immediatamente, oltre a una situazione caotica nei trasporti e una conseguente riduzione drastica degli introiti commerciali, un aumento della mortalità a seguito della carenza di acqua potabile e della mancata assistenza fornita dalle strutture ospedaliere coinvolte.[4]

Secondo Allianz Global il costo mondiale del crimine informatico si aggira intorno ai 450 miliardi di dollari l'anno, di cui le 10 principali economie mondiali rappresentano la metà del totale.[5] Numeri drammatici che mostrano un serio rischio per la stabilità del sistema finanziario e geopolitico mondiale. A questo si aggiunge la preoccupazione di alcuni analisti secondo cui le compagnie assicurative sottostimano i massimali dei danni aggregati. Infine non dobbiamo dimenticare che, a differenza di un'azienda, la sicurezza di uno Stato, che ha nelle infrastrutture critiche un suo punto nevralgico, non può ragionare esclusivamente in termini di danni economici. In un periodo in cui il concetto stesso di sicurezza nazionale deve fare i conti con il terrorismo, preoccupa sapere che nell'autunno 2015 lo US Office of Personnel Management ha ammesso che gli sono stati sottratti documenti inerenti la sicurezza nazionale tra cui più di 5 milioni di impronte digitali di impiegati federali.[6] Fatti come questo sottolineano l'importanza di una politica olistica di cyber security che non faccia eccessivamente riferimento al sistema assicurativo, per non correre il rischio di essere sì assicurati ma per nulla sicuri.

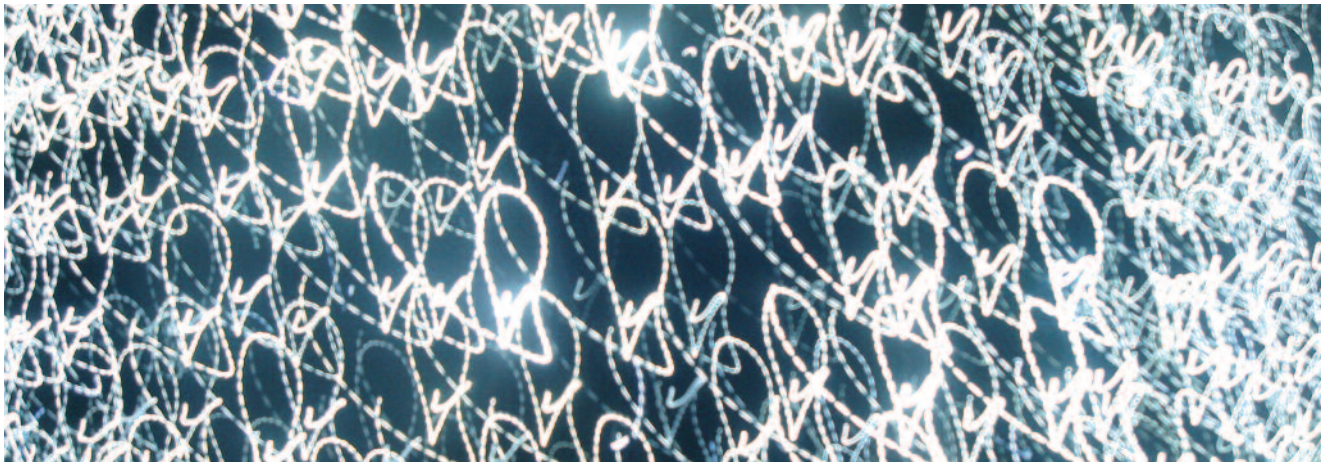
---

3 Healey J., Rohmeyer P., Sachs M. H., Schmidt J., Weiss J., Bayuk J. L., (2012), Cyber Security Policy Guidebook, New York, NY, Wiley.

4 Risk Management Solutions, Inc. Cambridge Centre for Risk Studies, (2016), Managing Cyber Insurance Accumulation Risk, in ‹ http://bit.ly/1pSXlJJ › (ultima consultazione 19-03-2016).

5 Allianz Global Corporate & Specialty, (2015), cit.

6 Sanger D. E., (2015), Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says, in The New York Times SEPT. 23, 2015, in ‹ http://nyti.ms/1G3gvOF › (ultima consultazione 19-03-2016).



Per evitare questo errore occorre partire dal presupposto che l'assicurazione entra in funzione solamente se le misure preventive hanno fallito. **Le assicurazioni sono da intendersi quindi come un tassello dell'analisi del rischio: un mosaico composto da fattori tecnici, organizzativi e legali, e solamente coniugando i vari aspetti in modo complesso e consapevole è possibile contrastare efficacemente il rischio, informatico e non solo.**
In tal proposito negli ultimi anni, il National Protection and Programs Directorate (NPPD) ha organizzato delle tavole rotonde invitando analisti assicurativi, brooker, risk manager, esperti informatici, gestori di infrastrutture critiche e scienziati sociali per esaminare lo stato del mercato assicurativo della sicurezza informatica e ragionando su come incentivare una migliore gestione del rischio. L'intento è di far interagire i protagonisti del settore pubblico e privato con lo scopo di proteggere le reti informatiche, assistendoli collettivamente e individualmente e migliorando così la sicurezza informatica complessiva.
Il report del NPPD ha identificato tre aree in cui sarebbe possibile ottenere una più robusta copertura, non solo per i danni economici e immateriali ma anche per quelli tangibili che coinvolgono le infrastrutture critiche. La prima ha a che fare con la necessità di condividere i dati degli attacchi informatici, una pratica poco diffusa perché mette a repentaglio l'immagine della sicurezza aziendale ma che può, tramite una condivisione anonima, creare un database di vitale importanza. Quest'ultimo potrebbe poi essere utilizzato dal settore assicurativo per costruire modelli di rischio e simulazioni più attendibili, così da stabilire un premio assicurativo preciso anche per sistemi complessi come le infrastrutture critiche. Infine, lo studio sottolinea la necessità di una diffusione capillare della cultura della gestione del rischio di impresa che limiti i fenomeni di contagio e riduca al minimo minimo il rischio residuo da trasferire sul mercato assicurativo.[7]
Uno dei primi fattori di cyber sicurezza su cui occorre lavorare è infatti interno alle aziende e ha a che fare con la formazione dei dipendenti. La maggior parte di questi sa poco di sicurezza informatica ed è probabile che inavvertitamente tenga comportamenti a rischio: un dipendente negligente che sbaglia a prendere le adeguate precauzioni espone costantemente il sistema. Negli ambienti assicurativi è noto il caso di Aon che durante una visita a un cliente ha scoperto che un quarto degli impiegati usava la password di default, che era appunto "password", e che quando è stata obbligata a cambiarla con un codice alfanumerico teneva la nuova password su un post-it sotto lo schermo del pc.

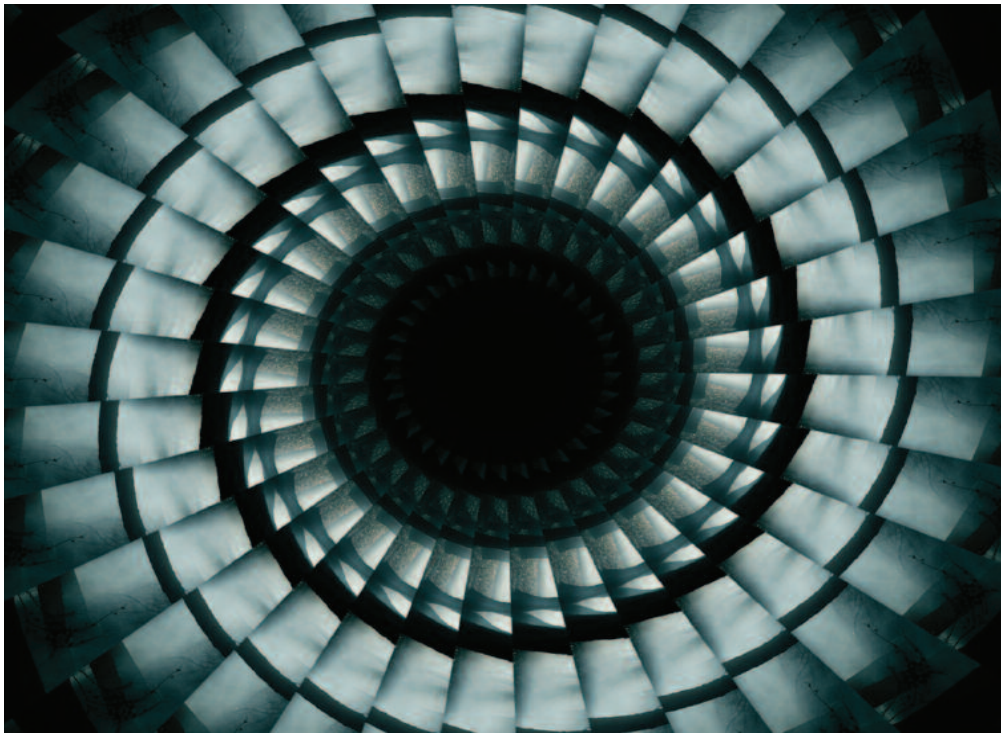
7 National Protection and Programs Directorate - The Department of Homeland Security, (2014), Insurance Industry Working Session Readot Report, in ‹ http://1.usa.gov/1nZC0wM › (ultima consultazione 19-03-2016).

Se si trasferisce una parte del rischio a una assicurazione occorre poi conoscere con precisione la reale copertura garantita dalla polizza. Secondo un report di Marsh più della metà dei CEO britannici ritiene che la propria polizza assicurativa copra anche il cyber risk aziendale, ma in realtà solamente il 10% rispetta del tutto questa aspettativa.[8] Secondo Adam Thomas di Deloitte & Touche LLP, a causa di superficiali calcoli di *pricing*, e del fatto che per avere modelli di rischio assicurativo attendibile occorrono almeno due decenni, il mercato delle cyber assicurazioni assomiglia a un "*wild wild west*" dove le aziende corrono il serio rischio di trovarsi con polizze che non forniscono una reale protezione ma addirittura una sensazione di illusoria sicurezza.[9]

Occorre quindi un piano olistico di analisi del rischio cyber che lavora su due livelli. Il primo è rappresentato dal cyber risk management e composto da interventi diversificati per la messa in sicurezza, in locale e in mobilità, in relazione a minacce esterne di natura informatica o di altro tipo. Il secondo livello consiste nel trasferimento dei rischi: visto che questi non sono del tutto eliminabili, i rischi residui vengono trasferiti con contratti ad hoc e finalizzati a far fronte al ripristino, alle perdite economico-finanziarie e alle pretese di terzi.

Per stimolare l'integrazione dei due livelli il legislatore può prendere a esempio i Certification Bodies introdotti nel Regno Unito: organismi che garantiscono l'implementazione delle procedure di sicurezza aziendale. Così come nella responsabilità civile auto una compagnia assicurativa può rivalersi sull'assicurato che non ha sottoposto il veicolo alla periodica revisione, allo stesso modo le società che intendono sottoscrivere una copertura cyber e devono garantire standard di sicurezza interni. Così facendo i meccanismi di rivalsa incentivano le aziende a un comportamento virtuoso creando un mercato assicurativo mirato ma anche limitando la diffusione sistemica del rischio. ■

8 Marsh, (2015), Cyber Risk Survey Report, in ‹ http://bit.ly/1H1aWWj › (ultima consultazione 19-03-2016).
9 Joyce S., (2016) These roadblocks are slowing down the cybersecurity insurance explosion, in Insurance Business America ‹ http://bit.ly/1Rrig2M › (ultima consultazione 19-03-2016).



CENTRO RICERCHE SOCIO-PSICOLOGICHE E CRIMINOLOGICO FORENSI

Il Centro Ricerche Themis nasce nel 2003 con il fine di promuovere lo studio, la ricerca e l'aggiornamento culturale nell'ambito delle scienze sociali, tecnologiche e della sicurezza.

Realizza inoltre prodotti editoriali con il marchio di **Edizioni Themis**.

Il Centro è diretto da Isabella Corradini.

isabellacorradini

Progetti e Ricerche

Themis realizza studi e ricerche negli ambiti della psicologia, della criminologia e della sicurezza (safety e security) privilegiando un approccio interdisciplinare. È inoltre specializzato nella costruzione di strumenti metodologici.

Seminari e Formazione

Il Centro Themis è partner di strutture qualificate per lo svolgimento di attività di formazione e seminari specialistici coerenti con le discipline trattate.

Pubblicazioni

Themis realizza prodotti editoriali a carattere specialistico negli ambiti della psicologia, del diritto, della criminologia, della salute e della sicurezza. I testi costituiscono strumenti di lavoro e di approfondimento impiegati anche in ambito accademico.

@ThemisRicerche

CentroRicercheThemis

themiscrime.com

PRIVACY E SICUREZZA: COME CAMBIA LO SCENARIO E I RIFERIMENTI NORMATIVI NEL NUOVO REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Graziano Garrisi

Manca poco, ormai, all'entrata in vigore del Nuovo Regolamento europeo sulla privacy, il quale apporterà alcune modifiche alla disciplina relativa alla protezione dei dati personali.
Uno dei campi in cui il Regolamento prevede delle novità è quello delle "**Misure di sicurezza**", sul quale vogliamo soffermare la nostra attenzione. Rispetto all'attuale Codice Privacy (D.Lgs. 196/2003), che prevede una bipartizione tra misure di sicurezza minime e idonee (le prime specificatamente individuate agli artt. 33-34 e all'Allegato B del Codice stesso, mentre le seconde non ben definite in quanto variano in base a una serie di parametri che devono essere valutati da ciascun titolare del trattamento), la normativa europea individua un corpus unico di misure di sicurezza che dovranno essere applicate tenendo conto dello stato dell'arte e dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento (compreso l'eventuale rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche).
Il nuovo regolamento europeo sulla protezione dei dati, infatti, prevede all'**art. 32**, che il titolare del trattamento e il responsabile del trattamento mettano in atto **misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**, che comprendono, tra le altre, altre, se del caso:

a) la **cifratura** dei dati personali e la **pseudonimizzazione**;
b) la capacità di assicurare su base permanente la **riservatezza**, l'**integrità**, la **disponibilità** e la **resilienza** dei sistemi e dei servizi di trattamento;
c) la **capacità di ripristinare** tempestivamente la disponibilità e l'accesso dei

Graziano Garrisi: Avvocato del Foro di Lecce dal 2008. Fa parte del Digital & Law Department dello Studio Legale Lisi, occupandosi principalmente di consulenza legale in materia di privacy e diritto delle nuove tecnologie, nonché nella realizzazione dei modelli organizzativi D. Lgs. 231/2001 e D.Lgs. 196/2003. Socio fondatore e membro del Direttivo di ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti) è Socio fondatore anche di ABIRT (Advisory Board Italiano dei Responsabili del Trattamento dei dati personali). Relatore in numerosi convegni e autore di pubblicazioni in materia di diritto delle nuove tecnologie. Iscritto all'elenco Anorc Professioni Responsabile Trattamento dei Dati Personali.

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).

dati personali in caso di incidente fisico o tecnico;

d) una procedura per **testare, verificare e valutare** regolarmente l'**efficacia delle misure tecniche e organizzative** al fine di garantire la sicurezza del trattamento.

A ben vedere, non si tratta di misure di sicurezza del tutto nuove rispetto al vecchio impianto normativo, soprattutto se le confrontiamo con i contenuti del Documento Programmatico sulla Sicurezza (noto anche come "DPS"), che costituiva una misura di sicurezza obbligatoria sino a qualche anno fa.

Una vera novità, invece, è rappresentata dalla "pseudonimizzazione" - che prevede che i dati personali non "possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" - e dall'utilizzo della "crittografia".

Occorre evidenziare, però, per non incorrere in errore, che il regolamento non impone – sempre o in qualunque caso - l'uso della pseudonimizzazione o della crittografia (l'utilizzo delle locuzioni "*tra le altre*" e "*se del caso*" è eloquente), ma obbliga i titolari o i responsabili del trattamento a valutare – caso per caso – quelli che possono essere i rischi inerenti a quello specifico trattamento e attuare, di conseguenza, misure per limitare tali rischi, come, ad esempio, proprio la cifratura e la pseudonimizzazione dei dati (come ribadito nella parte in cui si specifica "*per garantire un livello di sicurezza adeguato al rischio*"). Pertanto, è necessario effettuare, prima, un'analisi di rischio (in alcuni casi sarà necessaria una vera e propria "Valutazione d'impatto sulla protezione dei dati") e poi, se è il caso, adottare le misure di cifratura o pseudonimizzazione.

Le restanti indicazioni normative, invece, individuano i requisiti generici di sicurezza (es. sicurezza di reti e di sistemi d'informazione) che un sistema deve soddisfare per garantire la compliance privacy rispetto alla nuova regolamentazione europea e mettere in sicurezza tutto l'ambiente in cui l'informazione viene trattata:

- **riservatezza**, ovvero la protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la lettura da parte di persone non autorizzate;
- **integrità**, come conferma che i dati

trasmessi, ricevuti o conservati siano completi e inalterati;
- **disponibilità**, come conferma che i dati siano accessibili e i servizi funzionino anche in caso di interruzioni dovute a eventi eccezionali o ad attacchi di pirateria informatica.

Di dubbia interpretazione, invece, appare il termine "**resilienza**" (magari potremmo interpretarlo come obbligo di adottare misure volte a limitare l'impatto di un attacco a una serie di informazioni/dati o risorse, evitando il perpetrarsi di ulteriori danni, o come capacità di reazione di un sistema a fronte di un evento che metta a rischio la sicurezza delle informazioni e dei dati trattati), ma è facile comprendere come lo stesso sia strettamente legato anche alle ulteriori misure indicate alle lettere seguenti c) e d).

In particolare, il punto d) delle misure indicate all'art. 32, introduce quel principio di "rendicontazione" che prevede l'obbligo del Titolare del trattamento di conformarsi agli adempimenti derivanti dalla nuova normativa e di dimostrare tale conformità (e, quindi, il rispetto di tutti obblighi in capo allo stesso), anche mediante l'adozione di politiche interne e di meccanismi atti a garantire il rispetto del Regolamento stesso. Il titolare del trattamento, infatti, deve attuare i requisiti di sicurezza dei dati e mettere in atto meccanismi per assicurare la verifica dell'efficacia delle misure.

Ciò vuol dire che non solo si chiede al Titolare del trattamento (o al suo Responsabile) di adottare determinate misure di sicurezza (previa analisi dei rischi) e dimostrarne la conformità alla nuova regolamentazione europea, ma si chiede altresì di dimostrare che dette misure abbiano effettivamente funzionato durante il corso dei trattamenti effettuati (sulla scorta di quanto avviene nella redazione dei Modelli di Gestione e Organizzazione in base al D.Lgs. 231/2001).

Appare utile, infine, un confronto con le disposizioni previste, e ad oggi ancora vigenti, dal d.lgs. n. 196/2003 (Codice privacy). L'art. 31 stabilisce che *"i dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preven-*

tive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta". In più, ai sensi dell'art. 33 del Codice privacy, i titolari del trattamento sono tenuti ad adottare le **misure minime** volte ad assicurare un **livello minimo di protezione dei dati personali**. In particolare, per i trattamenti di dati effettuati con strumenti elettronici le misure di sicurezza idonee per garantire la sicurezza dei dati personali consistono "*nell'autenticazione informatica, nell'adozione di procedure di gestione delle credenziali di autenticazione, nell'utilizzazione di un sistema di autorizzazione, nell'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, nella protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici; nell'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi, nell'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari".*

Da una rapida comparazione, quindi, possiamo affermare che gli articoli dei due testi legislativi (italiano ed europeo, vecchia e nuova normativa) che affrontano la tematica delle "misure di sicurezza" non sono in antitesi, ma anzi, quanto riportato nel D.Lgs. 196/2003 costituisce la base e il punto di partenza per sviluppare un più completo "Data Protection Program" (sulla scorta del vecchio DPS), finalizzato a consentire al titolare del trattamento di dimostrare che ha adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici e idonei modelli organizzativi (in relazione ai trattamenti effettuati per le varie finalità perseguite e in base alle modalità e agli strumenti utilizzati). ■

ESTRATTO DEL "CYBER STRATEGY & POLICY BRIEF (VOLUME 03 – MARZO 2016)"

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

DANIMARCA

Il *Danish Defence Intelligence Service* (DDIS) è l'organo deputato a svolgere compiti di *intelligence* estera e militare per il governo danese. Inquadrato all'interno delle responsabilità istituzionali del Ministro della Difesa, il suo *Military Security Department* è incaricato delle attività di protezione delle Forze Armate da attacchi di spionaggio, sabotaggio, terrorismo e qualsiasi altra forma di attività criminale.
Inoltre, sin dalla sua creazione, avvenuta nel 2012, il *Danish Defence Intelligence Service* sovrintende e coordina anche le attività del *Centre for Cyber Security*: l'autorità indipendente deputata alla 'sicurezza cibernetica', il cui compito principale è quello di rilevare, segnalare e rispondere agli attacchi informatici condotti contro la sicurezza nazionale e gli interessi della Danimarca.
Seppure l'attuale approccio strategico danese – delineato da ultimo nella *cyber-strategy* del dicembre 2014 – preveda ancora una postura marcatamente difensiva, sin dal 2012 la *Danish Defence Commission* prima e il "*National Plan for Cyber Security*" del 2013 poi avevano evidenziato la necessità di incrementare e rafforzare le tecnologie e le capacità militari della Danimarca anche attraverso la creazione di una specifica unità militare per le attività offensive nel e attraverso il cyber-spazio.
Pertanto, nel gennaio del 2015, a seguito di una ulteriore esortazione in tal senso del Ministro della Difesa, il governo danese ha previsto di investire entro il 2017 circa 74 milioni di dollari per sviluppare le proprie capacità offensive sia militari, che di *intelligence* nel e attraverso il cyber-spazio.
Per raggiungere tale obiettivo, nel mese di marzo il governo danese ha dichiarato di aver costituto all'interno del *Danish Defence Intelligence Service* un'accademia completamente focalizzata sulla formazione dei propri esperti di 'sicurez-

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 Coordinatore dell'Osservatorio *InfoWarfare e Tecnologie emergenti* dell'Istituto Italiano di Studi Strategici 'Niccolò Machiavelli' e membro del International Institute for Strategic Studies. 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.

za cibernetica'. Il primo corso, della durata di 4 mesi e mezzo, avrà inizio ad agosto di quest'anno e si articolerà in moduli tesi ad approfondire tanto gli aspetti strategici e legali della materia, quanto soprattutto quelli tecnici inerenti sia le attività difensive, che offensive.
Il principale impiego di questi futuri esperti sembra essere attualmente legato più alle attività di spionaggio elettronico del *Danish Defence Intelligence Service*, che a quelle di *cyber-warfare* del suo *Military Security Department*. Tuttavia, il preciso e chiaro indirizzo politico in tal senso, nonché gli specifici compiti di protezione delle Forze Armate attribuiti al *Danish Defence Intelligence Service*, così come la presenza al suo interno del *Centre for Cyber Security*, fanno propendere nel breve periodo verso lo sviluppo di percorsi di formazione legati anche alle capacità offensive strettamente militari e non solo a quelle di *intelligence*.
Come ampiamente delineato nel ***"Cyber Strategy & Policy Brief"*** **di gennaio 2016** e più avanti in questo volume (si veda, ad esempio, la parte relativa agli Stati Uniti), l'azione del governo danese appare assolutamente in linea con l'approccio strategico di un numero sempre maggiore di Stati a livello internazionale, che ormai da oltre un anno hanno cominciato a concentrarsi sempre più sullo sviluppo di capacità offensive nel e attraverso il cyber-spazio, tanto per scopi di *intelligence*, quanto per vere e proprie attività di *cyber-warfare*.

STATI UNITI

Come approfondito anche nel "***Cyber Strategy & Policy Brief***" **di gennaio 2016**, gli Stati Uniti continuano a spingere sull'acceleratore dello sviluppo delle proprie capacità militari offensive per il cyber-spazio.
Nel mese di marzo, il corpo dei *Marine* ha istituito il suo *Marine Corps Cyberspace Warfare Group*.
La principale missione di questo *Gruppo* – già oggi attivo, ma che raggiungerà la piena operatività solo nel 2017 – è quella di addestrare, rafforzare ed equipaggiare le unità operative dei *Marine* incaricate di svolgere missioni sia difensive, che offensive nel e attraverso il cyberspazio a supporto dello *United States Cyber Command* e del *Marine Forces Cyberspace Command*.
Costituito nell'ottobre del 2009, il *Marine Corps Forces Cyberspace Command* è, infatti, uno dei quattro pilastri che contribuiscono a formare lo *United States Cyber Command*, insieme al *Navy Fleet Cyber Command/10th Fleet*, l'*Army Cyber Command/2nd Army*, e l'*Air Forces Cyber Command/24th Air Force*.
Delle 123 unità operative e i 4.990 uomini per le operazioni militari nel e attraverso il cyber-spazio attualmente in forza allo *United States Cyber Command*, sono 13 le unità messe finora in campo dal *Marine Corps Forces Cyberspace Command*, di cui una già certificata come "*Full Operational Capability*".
Esse conducono operazioni nel cosid-

detto "quinto dominio della conflittualità" nell'intero spettro delle operazioni militari e dispiegano una forza di 1000 uomini tra personale dei *Marine* e civili, che dovrebbe salire a circa 1300 uomini proprio entro la fine del 2016.
Ciò non di meno, la previsione del governo è di riuscire ad avere, entro la fine del 2017, tutte le 13 unità del *Marine Corps Forces Cyberspace Command* certificate come "*Full Operational Capability*". Ciò comporterà quindi che, entro la fine del prossimo anno, il *Marine Corps Forces Cyberspace Command* fornirà allo *United States Cyber Command* ben 1 *Cyber National Mission Team*, 3 *Cyber Mission Team* con 1 *Cyber Support Team* e 8 *Cyber Protection Team* (di cui 3 completamente dedicati alle sole esigenze del corpo dei *Marine*).
Tuttavia, il corpo dei *Marine* non è l'unico ad essere impegnato nello sviluppo delle proprie capacità per il cyber-spazio. Sempre nel mese di marzo, infatti, anche l'*Air Force Space Command* americano ha annunciato che il proprio sistema di arma denominato "*Cyberspace Vulnerability Assessment/Hunter Weapon System*" ha raggiunto lo *status* di "*Full Operational Capability*".
A dispetto del nome, questa piattaforma è deputata esclusivamente alla difesa dei sistemi informatici dell'*Air Force* e al supporto degli *United States Cyber Command Cyber Protection Team* e consente di svolgere principalmente *vulnerability assessment* e valutazione di conformità dei sistemi, ma anche attività di vera e propria rilevazione delle minacce informatiche provenienti dall'esterno. La parte denominata *Hunter*, infatti, consente di identificare, mitigare e perseguire – entro i confini della rete dell'*Air Force* – le minacce informatiche provenienti dall'estero che mirano a colpire le capacità operative di questa Forza Armata e dello *United States Cyber Command*.
Sotto il punto di vista strettamente governativo, invece, alla notizia dello US-CERT che nel 2015 i sistemi informatici del governo americano hanno sofferto ben 77.183 incidenti informatici (il 10% in più rispetto all'anno precedente), ha fatto eco il Presidente Obama, che il 29 marzo, attraverso una lettera al Congresso, ha esteso l'efficacia dell'ordine esecutivo emanato ad aprile del 2015 dal titolo: "*Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*".
Seppure, allo stato attuale, quest'ordine esecutivo non abbia ancora mai trovato reale applicazione, la recente accusa formale del Dipartimento della Giustizia americano nei confronti di un gruppo di sette iraniani, imputati di aver condotto – tra il 2011 e il 2013 – una campagna

coordinata di attacchi informatici contro il settore finanziario degli Stati Uniti (per il cui approfondimento si rimanda al paragrafo successivo), unita all'immediato annuncio da parte di Obama dell'estensione dell'efficacia di quest'ordine esecutivo, parrebbero presagire che il governo americano stia valutando la possibilità di emanare sanzioni economiche nei confronti del governo di Teheran a seguito di questi attacchi informatici.
In conclusione, il governo americano continua ad estendere la sua azione politica e strategica per il cyber-spazio seguendo due principali direttrici. La prima, più marcatamente istituzionale, sempre più tesa a rinforzare le difese dei sistemi informatici del governo e ad aumentare la consapevolezza di queste materie in tutti gli strati del suo tessuto sociale (per il cui approfondimento si rimanda anche al ***"Cyber Strategy & Policy Brief"* di febbraio 2016**).
La seconda direttrice, invece, più marcatamente militare e di *intelligence*, che vede gli Stati Uniti impegnati a ritmi serrati nel continuare a sviluppare le loro capacità offensive per il cyber-spazio e a dimostrare pubblicamente di essere in procinto di risolvere il problema dell'anonimato e dell'incapacità di attribuire un attacco informatico ai suoi autori materiali. Ciò, anche al fine di generare deterrenza negli Stati nemici e negli alleati.

STATI UNITI – FOCUS SULLA CYBER-DETERRENZA (DALLA SYRIAN ELECTRONIC ARMY, AGLI HACKER DI STATO IRANIANI E CINESI)

Sin dal 2011, la *Syrian Electronic Army*, un gruppo di attivisti informatici che supporta il governo di Bashar Al-Assad, ha fatto ripetutamente parlare di sé per i numerosi cyber-attacchi portati a segno soprattutto nei confronti di agenzie di stampa e società tecnologiche occidentali.
Seppure il valore tecnico di questi attacchi non abbia mai raggiunto livelli preoccupanti, gli effetti di alcuni di essi sono riusciti a causare danni a volte anche molto rilevanti.
Tra tutti, il principale attacco informatico realizzato dalla *Syrian Electronic Army* è senza dubbio quello del 2013 all'*account* Twitter ufficiale dell'agenzia di stampa *Associated Press*. Grazie alla sua compromissione, infatti, utilizzando un singolo *tweet* che annunciava la notizia falsa di due esplosioni alla Casa Bianca e il ferimento di Barack Obama, questo gruppo di 'hacktivisti' è riuscito a far perdere 136,5 miliardi di dollari all'indice azionario *Standard&Poor 500*. Una cifra decisamente ragguardevole, considera-

to soprattutto che è stata persa nei tre minuti necessari a capire che nessun'altra agenzia di stampa stava battendo e confermando quella notizia e che quindi quel *tweet* annunciava in realtà un'informazione completamente falsa.
Nel mese di marzo, però, la *Syrian Electronic Army* è tornata a far parlare di sé non a seguito di ulteriori attacchi informatici, ma in conseguenza dell'annuncio da parte del governo americano di aver individuato e aggiunto due dei suoi principali membri nella lista dell'FBI dei maggiori ricercati per crimini informatici. Ahmad Umar Agha (22 anni, siriano di Damasco, conosciuto su Internet come "The Pro") e Firas Dardar (27 anni, siriano di Homs, conosciuto su Internet come "The Shadow") sono i nomi dei due membri della *Syrian Electronic Army* nei cui confronti l'FBI ha emanato una ricompensa di 100.000 dollari ciascuno nel caso in cui qualcuno fornisca informazioni che dovessero portare al loro arresto.
Inoltre, sempre nel mese di marzo e quasi contemporaneamente a questa vicenda, il Dipartimento della Giustizia americano ha formalmente accusato un gruppo di ben sette iraniani, impiegati in due aziende operanti per il governo di Teheran e il suo *Islamic Revolutionary Guard Corps*, per aver condotto – tra il 2011 e il 2013 – una campagna coordinata di attacchi informatici contro il settore finanziario degli Stati Uniti. Oltre a questo, per uno dei sette iraniani l'accusa è anche di aver abusivamente guadagnato più volte l'accesso ai sistemi informatici di comando e controllo di una diga di New York.
Invero, occorre precisare che gli Stati Uniti non sono nuovi a questo genere di iniziative.
Già nel maggio del 2014, infatti, sempre il Dipartimento della Giustizia americano aveva formalmente accusato di spionaggio elettronico cinque membri della '*Unità 61938*' della *People's Liberation Army* (PLA) cinese per aver violato i si-

stemi informatici di sei aziende americane alla ricerca di segreti industriali.
Seppure sul piano puramente processuale sembra ovviamente poco probabile che qualcuno degli accusati comparirà mai dinanzi ad una corte degli Stati Uniti, sul piano politico e strategico, invece, l'obiettivo di Washington appare essere molto chiaro e coerente.
Infatti, cominciando a perseguire formalmente gli autori materiali dei crimini informatici di natura statale o sponsorizzati da uno Stato, il governo americano ha anzitutto iniziato a dimostrare pubblicamente le proprie capacità di rintracciare gli autori di quegli attacchi. Ciò significa mandare a livello internazionale il messaggio di stare risolvendo il principale problema nel settore della *cyber-security*, ovvero l'anonimato e l'incapacità di attribuire con certezza la responsabilità di un attacco informatico ai suoi autori materiali.
Peraltro – ed è questo un ulteriore elemento fondamentale – l'acquisizione di questa capacità concorre a colmare uno dei principali "vuoti" per il rafforzamento di una strategia di deterrenza per il cyber-spazio che sia realmente efficace.
Le peculiarità della rete Internet, infatti, impongono al momento di guardare in maniera "tiepida" nei confronti della reale possibilità di attuare una strategia di deterrenza.
Proprio il problema dell'anonimato e della notevole difficoltà nel riuscire a risalire con certezza a chi realmente ha la responsabilità dell'attacco (mancanza dell'elemento difensivo della deterrenza), unito alla conseguente impossibilità di poter contrattaccare all'attacco informatico subìto (mancanza dell'elemento offensivo della deterrenza) e alla relativa tranquillità e affidamento da parte di chi attacca sulla mancanza di questi due elementi (mancanza dell'elemento della paura), fa scaturire, come detto, una generica e diffusa difficoltà per gli Stati nel costruire una strategia di deterrenza per il cyber-spazio che sia davvero efficace.
Tuttavia, riuscendo a risolvere il problema dell'anonimato (seppure – almeno al momento – con tempi ancora abbastanza lunghi) e contestualmente continuando a consolidare la propria *leadership* internazionale nelle operazioni militari e di *intelligence* nel e attraverso il cyber-spazio (peraltro per mezzo di una postura sempre più marcatamente offensiva), gli Stati Uniti ben presto riusciranno a generare deterrenza in maniera molto efficace anche nel cosiddetto "quinto dominio della conflittualità", consolidando così ancor di più il loro ruolo di maggiore "cyber-potenza" a livello globale.
Per ulteriori approfondimenti e aggiornamenti sulla strategia degli Stati Uniti, si veda anche lo specifico paragrafo in questo volume e il "***Cyber Strategy & Policy Brief***" di gennaio 2016. ■

LA FIRMA ELETTRONICA AVANZATA (FEA) NEL REGOLAMENTO UE N. 910/2014 (EIDAS)

Giovanni Manca,
Membro del comitato scientifico di AIFAG

PREMESSA

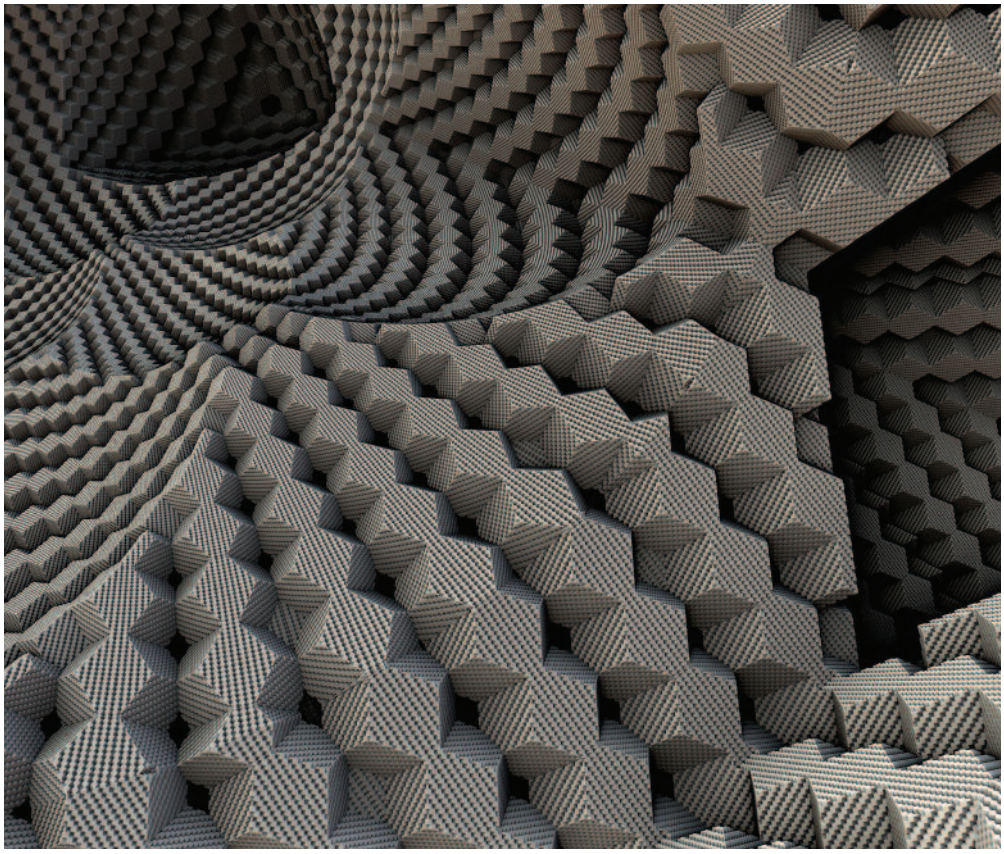
La firma elettronica avanzata (FEA) è stata introdotta dalla direttiva 1999/93/CE come base per la firma elettronica qualificata. Questa è realizzata se alla FEA si aggiungono un cosiddetto certificato qualificato e la firma viene creata utilizzando un "dispositivo sicuro" che nei fatti è un apparato che possiede specifiche e ben determinate caratteristiche di sicurezza.
Nel vigente Codice dell'amministrazione digitale alla FEA viene attribuita una efficacia probatoria quasi uguale a quella di una firma qualificata. Questa circostanza ha determinato una elevata diffusione di soluzioni di FEA basate sulla tecnologia biometrica della sottoscrizione autografa. Il Regolamento UE 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (eIDAS) non ha impatti sulla efficacia probatoria della normativa italiana.
Peraltro con la Decisione di Esecuzione 2015/1506 della Commissione dell'8 settembre 2015 vengono stabilite le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati
(ai sensi dell'eIDAS un sigillo elettronico è definito come "*dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi*") che gli organismi del settore pubblico devono riconoscere.
Questo per garantire le regole ai fini dell'applicazione all'articolo 27, paragrafo 5 e all'articolo 37, paragrafo 5 del Regolamento eIDAS. Di quanto stabilito in questa decisione e degli impatti sull'ordinamento nazionale si parla nei paragrafi seguenti.

LA FEA NEL REGOLAMENTO EIDAS

Nel Regolamento eIDAS la FEA è introdotta nell'articolo 3, numero 11) con un rinvio immediato all'articolo 26.

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).



Qui vengono stabiliti i requisiti che una FEA deve soddisfare:

a) è connessa univocamente al firmatario;
b) è idonea a identificare il firmatario;
c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

E' positivo il fatto che tali requisiti siano praticamente identici a quelli della direttiva 1999/93/CE che il Regolamento eIDAS abroga dal 1 luglio 2016.

In termini di efficacia probatoria il Regolamento eIDAS non si esprime perché non competente in termini di Diritto comunitario, quindi rimane valido quanto stabilito nel CAD.

La Decisione di esecuzione 2015/1506 è cruciale per definire il quadro degli strumenti tecnici necessari ad un trattamento transfrontaliero delle firme e dei sigilli elettronici avanzati.

LA DECISIONE DI ESECUZIONE 2015/1506

Questa norma secondaria del Regolamento eIDAS è stata promulgata (come evidenziato nel *considerando* (1)) in quanto *"è indispensabile che gli Stati membri si dotino degli strumenti tecnici necessari al trattamento dei documenti firmati elettronicamente che sono richiesti quando si utilizza un servizio online offerto da un organismo del settore pubblico o per suo conto".*

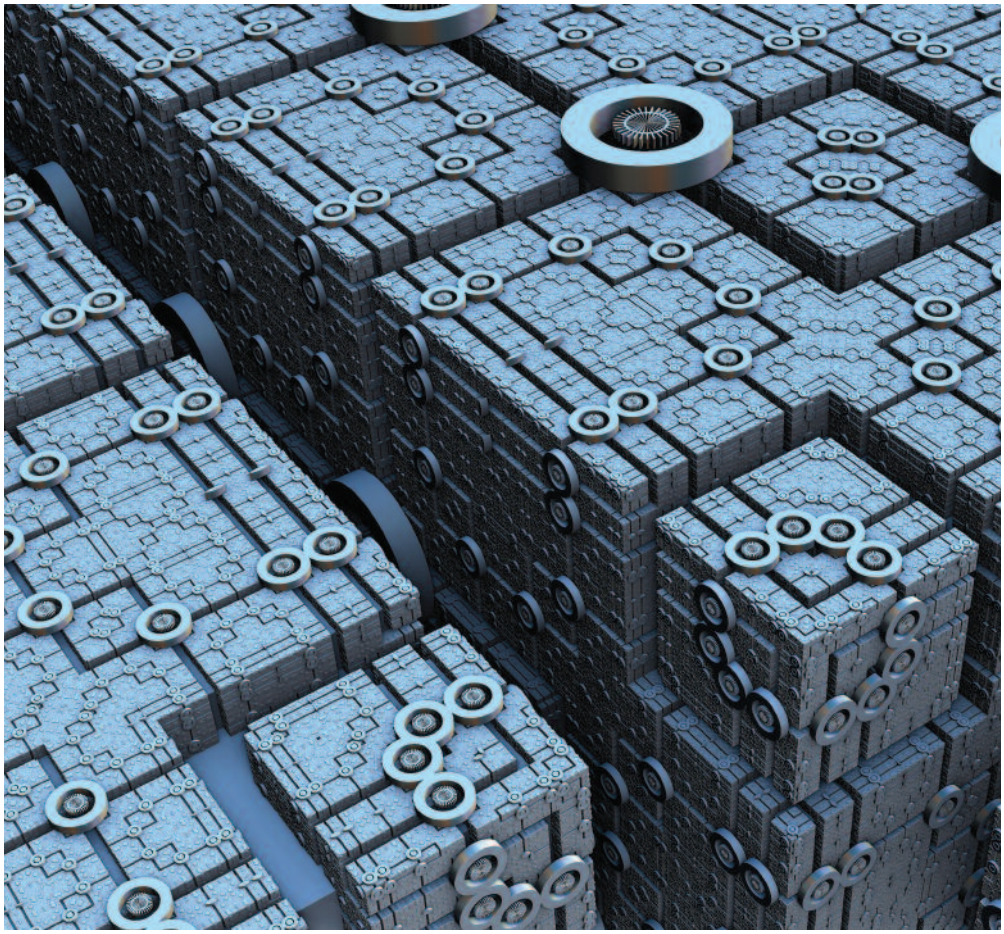
Il Regolamento eIDAS obbliga gli Stati membri che richiedono una FEA per l'uso di un servizio online offerto da un organismo del servizio pubblico, o per suo conto, a riconoscere le firme avanzate, le firme avanzate basate su un certificato qualificato e le firme qualificate che hanno formati specifici o formati alternativi convalidati conformemente a specifici metodi di riferimento.

Quanto detto per le firme deve essere applicato in modo analogo per i sigilli elettronici in quanto questi due oggetti sono simili dal punto di vista tecnico.

Ai fini dell'interoperabilità transfrontaliera in termini di verifica delle firme e dei sigilli devono essere utilizzati i formati definiti nella sopra citata Decisione della Commissione.
Ma nei casi dove per l'apposizione di una firma o di un sigillo vengano utilizzati formati di firma elettronica o di sigillo elettronico diversi da quelli comunemente supportati dal punto di vista tecnico, dovrebbero essere forniti mezzi di convalida che consentano la verifica transfrontaliera di tali firme o sigilli. Lo Stato membro ricevente deve poter fare affidamento sugli strumenti di convalida di un altro Stato membro, quindi è necessario fornire informazioni facilmente accessibili su tali mezzi mediante l'inserimento nei documenti informatici, nelle firme o nei contenitori dei documenti elettronici. (Per i contenitori con firma associata si deve fare riferimento alla specifica tecnica ETSI TS 103 174 v.2.2.1).
Infine è utile ricordare l'articolo 2, paragrafo 1 della Decisione in esame
1. Gli Stati membri che richiedono una firma elettronica avanzata o una firma elettronica avanzata basata su un certificato qualificato, secondo quanto disposto dall'articolo 27, paragrafi 1 e 2, del Regolamento (UE) n. 910/2014, riconoscono formati di firma diversi da quelli di cui all'articolo 1 della presente decisione, a condizione che lo Stato membro in cui è stabilito il prestatore di servizi fiduciari utilizzato dal firmatario offra agli altri Stati membri possibilità di convalida della firma, idonee ove possibile al trattamento automatico.
Per concludere la descrizione delle specifiche tecniche si deve citare l'obbligo di riconoscimento per gli Stati membri che richiedono una FEA o una FEA basata su un certificato qualificato delle specifiche tecniche in allegato alla Decisione in esame 2015/1506.
Le specifiche di FEA sono per XML, CMS o PDF al livello di conformità B. T o LT (è utile ricordare che tali livelli di conformità sono descritti nelle citate specifiche ETSI. B sta per Basic, T per Trusted time for signature existence e LT per Long Term with archive time-stamps) o tramite il già citato contenitore con firma associata.
Nell'allegato della Decisione sono riportati gli estremi delle specifiche tecniche ETSI alle quali è fatto obbligo di attenersi.

CONSIDERAZIONI FINALI

Il quadro comunitario che si va a configurare è quello di una serie di regole transfrontaliere aventi lo scopo di garantire lo scambio di documenti informatici tra Stati membri con il supporto di adeguate regole di verifica delle firme e dei sigilli per l'interoperabilità.
L'efficacia probatoria della FEA stabilita nel CAD non è influenzata dalle norme UE quindi i progetti di FEA basati su tecnologie biometriche di firma grafometrica non sono influenzati dall'eIDAS.
L'intercambio transfrontaliero di FEA grafometriche si scontra con una serie di problematiche di non facile soluzione.
Prima di tutto è indispensabile sottolineare il fatto che l'efficacia probatoria della FEA è di natura esclusivamente nazionale. Lo Stato membro mittente può inviare una FEA grafometrica in Italia ma la verifica completa sarebbe possibile solamente a seguito di richiesta dell'Autorità giudiziaria (Provvedimento prescrittivo 513/2014 del Garante per la protezione dei dati personali).
Questo è un limite che può essere superato mediante accordi specifici tra le parti, ma se il foro competente fosse fuori dall'Italia avremmo dei rischi in giudizio che devono essere attentamente valutati.
In ogni caso è utile sviluppare uno standard di interoperabilità europeo in ambito ETSI partendo dalle regole ISO/IEC 19794-7 per la firma biometrica.
In tal modo ogni firma biometrica, nelle more della richiesta dell'Autorità giudiziaria, sarebbe verificabile con tutti gli strumenti di verifica conformi all'ipotizzato standard ETSI.
Per firme e sigilli avanzati conformi alle specifiche tecniche pubblicate nell'allegato della Decisione 2015/1506 è possibile procedere senza alcun problema tecnico o normativo fatto salvo quanto stabilito in eiDAS negli articoli 27 e 37 per i sigilli elettronici. ■



Gestire il cambiamento del software nel sistema informativo sanitario

Se paragonassimo l'Azienda sanitaria ad un corpo umano, il software ne rappresenterebbe il sistema nervoso centrale. Piccoli cambiamenti su tale componente avrebbero enorme impatto sugli organi dell'intero sistema causando rallentamenti, blocchi delle funzionalità, mancanza di coordinamento e potenziali danni irreversibili. Una progettazione ed una gestione errata del software potrebbero produrre problematiche di varia entità che, sia valutate singolarmente che in maniera olistica, andrebbero a costituire una seria minaccia al funzionamento generale del sistema. Di conseguenza risulta fondamentale proteggere questo asset core adottando specifiche attenzioni, evitando così incidenti e possibili situazioni di crisi.

Negli ultimi anni la centralizzazione dei servizi e dei sistemi informatici della Pubblica Amministrazione ha comportato da un lato una diminuzione generale degli incidenti, dall'altro un aumento della criticità dei sistemi stessi e della superficie di impatto intesa come entità degli eventuali danni. Il potenziamento e la ridondanza delle infrastrutture elettriche, con l'evoluzione e l'au-

Giampaolo Franco: Laureato in Informatica è certificato CISM. Da più di 10 anni esperto di governance, risk management, and compliance presso l'Azienda Provinciale per i Servizi Sanitari di Trento. Si occupa di svolgere le attività inerenti alla business continuity ed al disaster recovery, analisi dei rischi, privacy compliance, awareness, internal/external audit, incident management, ottimizzazione e controllo di qualità dei processi IT. In passato ha svolto attività di project management, analisi e programmazione di software in ambito bancario. E' stato consulente dell'Università di Trento nella definizione degli aspetti organizzativi e di sicurezza legati all'introduzione di modelli integrati di didattica digitale nella scuola. Conduce con passione attività di ricerca, formazione ed awareness nell'ambito della sicurezza rivolte alla pubblica amministrazione. Dal 2014 è membro dell'ISACA VENICE Chapter.

mento di velocità e resilienza delle reti di comunicazione, ha eliminato sensibilmente gli incidenti relativi a blackout elettrico ed indisponibilità del collegamento di rete. Di conseguenza il focus delle problematiche si è spostato ad un livello più alto: il software.

Il software è una componente molto costosa che frequentemente va aggiornata, risulta sempre più complessa, interdipendente ed indispensabile. Necessita di protezione e monitoraggio in quanto presente in tutti i livelli e processi aziendali e in quanto parte più onerosa dei servizi informatici. Grazie ad esso le strutture interne ed esterne delle Aziende sanitarie hanno raggiunto un livello di controllo ed automazione mai visto prima. Le nuove tecnologie di diagnostica strumentale, la condivisione delle informazioni sanitarie tra professionisti di strutture diverse, la dematerializzazione dei certificati di malattia e delle prescrizioni farmacologiche, la telemedicina, nonché i sofisticati sistemi automatici di monitoraggio ed allarme continuano ad apportare notevole beneficio all'utenza Aziendale. Può sembrare strano, ma l'utilizzo del software presenta delle problematiche intrinseche ed in prima battuta di difficile risoluzione. Semplici aggiornamenti, ad esempio, possono creare blocchi parziali o totali di funzionamento ed anche perdite di dati. E' per questo motivo che un processo coordinato di supervisione e gestione dei cambiamenti software risulta indispensabile. Sebbene già da tempo sia stata posta attenzione ad alcuni aspetti di sicurezza, quali la tutela della privacy ed il rischio clinico, in quanto previsti dalla legge e quindi obbligatori, manca una corretta gestione del cambiamento del software: non esistono infatti nelle Aziende sanitarie dei processi e delle figure ad hoc. Un miglioramento in tal senso renderebbe l'Azienda più in grado di interpretare il contesto di cambiamento tecnologico, ottimizzando i costi gestionali e disponendo più correttamente le risorse. In tal modo, gli incidenti sugli asset core dovrebbero mostrare una significativa diminuzione. Non agendo su questo asset i potenziali danni, sia relativamente al settore umano (pazienti, operatori) che tecnologico (dati d'archivio), possono risultare non più circoscrivibili ad un livello accettabile.

GIAMPAOLO FRANCO

Azienda Provinciale per i Servizi Sanitari di Trento

L'esternalizzazione della gestione hardware e software spesso comporta una gestione incompleta del risk assessment periodico, un'adozione di procedure di comunicazione insufficienti ed un carente monitoraggio e controllo preventivo e detettivo. Una banale minaccia informatica potrebbe sfruttare queste vulnerabilità e generare anche un security incident. Dal momento che le informazioni trattate dai sistemi informativi sanitari possono essere catalogate come 'supersensibili', in quanto riferite direttamente alla salute della persona, risulta ancor più necessario adottare e mantenere alti livelli di sicurezza e qualità nella gestione dei dati e dei processi, istituendo specifiche misure di protezione che tengano conto delle tecnologie, delle interdipendenze tra servizi e delle finalità. La perdita di qualità dei dati ha un'inevitabile ricaduta trasversale nell'organizzazione, creando un effetto domino di forte impatto negativo dal punto di vista dell'erogazione dei processi e della salute dei pazienti. Tale propagazione di errore andrebbe evitata adottando contromisure organizzative aziendali, coinvolgendo maggiormente il reparto IT, obbligando le terze parti a misure di controllo ed audit tramite strumenti giuridico/contrattuali ed implementando processi organizzativi e framework tecnologici orientati alla sicurezza. La gestione del cambiamento del software andrebbe monitorata centralmente e configurata come attività on-going e non one-time, dedicando personale qualificato a definire obiettivi di sicurezza, politiche del cambiamento tecnologico, standard e linee guida aziendali.

Il referente tecnologico delle Unità Operative dovrebbe acquisire le competenze del Change Manager per interfacciarsi con il Risk Manager e l'Information Security Manager. La politica aziendale dovrebbe inoltre essere orientata verso la gestione del post-cambiamento per raccogliere e gestire i feedback degli utenti ai fini del miglioramento continuo. Le problematiche riscontrate in tal modo verrebbero indirizzate dai professionisti ai rispettivi stakeholders misurando il grado culturale degli stessi. La cultura del personale interno e dei fornitori risulta una componente essenziale intrinseca ad ogni processo, a cui va posta particolare attenzione.

La logica di business, utilizzata da controparti esterne, normalmente differisce da quella dell'Azienda sanitaria; ciò comporta dei rischi, dovuti al gap culturale, che possono precludere la creazione di partnership professionali inclini alle buone pratiche di sicurezza. Per evitare ciò è necessario un team dedicato altamente competente che predisponga opportuni processi di gestione del rischio delle terze parti.

La consapevolezza di queste tematiche potrebbe crescere ed espandersi in maniera capillare, per improntare un livello culturale ed un clima aziendale incline alle buone pratiche di gestione del cambiamento tecnologico. La sicurezza non verrebbe più vista come costo e pesante responsabilità, ma verrebbe rivalutata come obiettivo e valore aggiunto.

Ogni servizio erogato dall'Azienda sanitaria è costituito, oltre che dal software, anche da ulteriori asset molto onerosi quali i professionisti utilizzatori, l'hardware, le infrastrutture di rete. Dal punto di vista dell'analisi dei rischi, ognuna di

queste componenti presenta tre caratteristiche fondamentali:

- CONFIDENTIALITY. Confidenzialità è l'equivalente di riservatezza o più semplicemente privacy. Le misure adottate per assicurare la confidenzialità servono a prevenire che informazioni riservate e sensibili vengano consultate da persone non autorizzate.
- INTEGRITY. Integrità significa mantenere la consistenza, la precisione e l'attendibilità dei dati nel loro intero ciclo di vita. I dati non possono essere cambiati da nessuna componente del servizio senza una specifica autorizzazione né alterati a causa di errori.
- AVAILABILITY. Disponibilità significa garantire rigorosamente la continuità ed il corretto funzionamento dei processi che gestiscono le informazioni. I dati devono essere disponibili agli utenti secondo i Service Level Agreement - SLA garantiti dal fornitore o dall'Azienda.

Il livello di sicurezza di ogni asset dipende quindi dalla somma di questi tre parametri. Qualsiasi atto di violazione di un'esplicita od implicita politica di sicurezza aziendale basata su queste tre componenti si definisce incidente di sicurezza. Le casistiche principali in cui si verifica un incidente di sicurezza possono essere così riassunte:

- Tentativi non autorizzati per guadagnare accesso ai dati ed ai sistemi;
- interruzioni di servizio inattese a causa di guasti od errori;
- interruzioni deliberate della indisponibilità dei servizi;
- uso non autorizzato di un sistema per processare o memorizzare dati;
- cambiamenti alle caratteristiche di un sistema hardware, firmware o software senza che il proprietario ne sia a conoscenza, o che non abbia fornito istruzioni in tal senso ed opportuno consenso.

Gli aggiornamenti software rientrano tra le cause principali di incidente di sicurezza. Al fine di ridurre i costi di Information Technology ed abbattere il rischio tecnologico, mitigare il rischio dovuto alla frequente attività di aggiornamento del software permetterebbe di governare in maggior sicurezza il sistema informativo sanitario e proteggere il raggiungimento degli obiettivi aziendali. ■

SUGGERIMENTI BIBLIOGRAFICI

Application security ISO/IEC 27034:2011. International Organization for Standardization (ISO) - International Electrotechnical Commission (IEC).

Agenzia per l'Italia Digitale (2013): Linee Guida per la razionalizzazione della infrastruttura digitale della Pubblica Amministrazione. Presidenza del Consiglio dei Ministri.

European Commission - DG CONNECT (2015): eHealth projects Research and Innovation in the field of ICT for Health and Wellbeing: an overview. Digital Agenda for Europe.

PA Consulting Group (2015): Security for industrial control systems - Manage third party risks - A good practice guide 12/5/2015. CNPI - Centre for the Protection of National Infrastructure; CESG – Communications - Electronics Security Group UK.

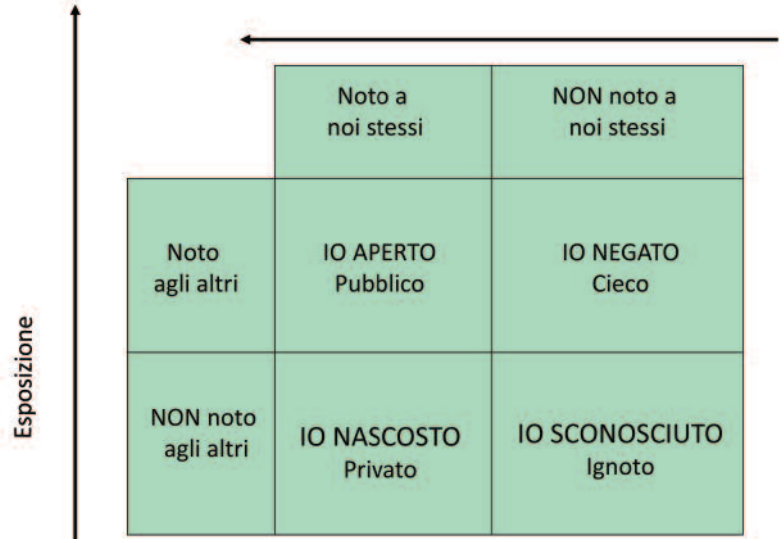
Paul Cichonski, Tom Millar, Tim-Grance, Karen Scarfone (2012): Computer Security Incident Handling Guide. National Institute of Standards and Technology – NIST.

Johari e la Privacy

Cosa c'entrano i Sigg. Johari e la Privacy o meglio la gestione del dato personale?
E cosa è la finestra di Johari?
Da Wikipedia: *Lo Schema di Johari (o Johari Window) è stato inventato nel 1955 da Joseph Luft e Harry Ingham, che hanno combinato le iniziali dei loro nomi. Il riferimento concettuale dello schema è collegato ad aspetti di comunicazione interpersonale e alla dinamica di gruppo. Esso definisce le relazioni interpersonali tra persone in quattro quadranti basati su due dimensioni. Lo schema è composto da un quadrato, suddiviso in quattro quadranti. Nella dimensione orizzontale si misura il grado di conoscenza che la persona ha di sé stesso in termini di personalità, atteggiamenti, impressioni ed emozioni trasmesse agli altri. Quest'ultimo tipo di conoscenza può pervenire alla persona solo dall'esterno: per questo un modo di identificare il valore su questa scala è la frequenza con cui il soggetto chiede esplicitamente un feedback agli altri sul suo comportamento e sulle impressioni che ha generato. La misura verticale invece si riferisce al grado di conoscenza che gli altri hanno del soggetto. La combinazione di queste due mi-*

Stefano Gorla: È nato a Milano, (classe 1962) si è laureato in fisica nucleare presso l'Università di Padova. Ha insegnato per qualche anno Matematica e Fisica presso alcuni licei. Attualmente è Privacy Busniss Unit Director c/o una primaria società di consulenza e consulente in contesti aziendali, istituzionali e dei servizi per la tutela del dato personale e della conservazione. Formatore accreditato (AIF e Aicq) in ambito tutela del dato personale e conservazione a norma documentale. Delegato regionale per la Lombardia di ANDIP (Associazione Nazionale per la Difesa della Privacy), socio A.N.F.I (Associzione Nazionale Finanzieri)e Esaminatore/Componente commissione Deliberante CERSA per lo schema Privacy. Ha maturato notevoli esperienze come Responsabile Qualità e Ambiente c/o aziende nei settori servizi e precedentemente come Qualità System Manager e Responsabile di un laboratorio di ricerca/linea pilota per componenti optoelettronici. E' autore di varie pubblicazioni sul tema su riviste specializzate, autore di libri e articoli di privacy, energia, astronomia, cosmologia.

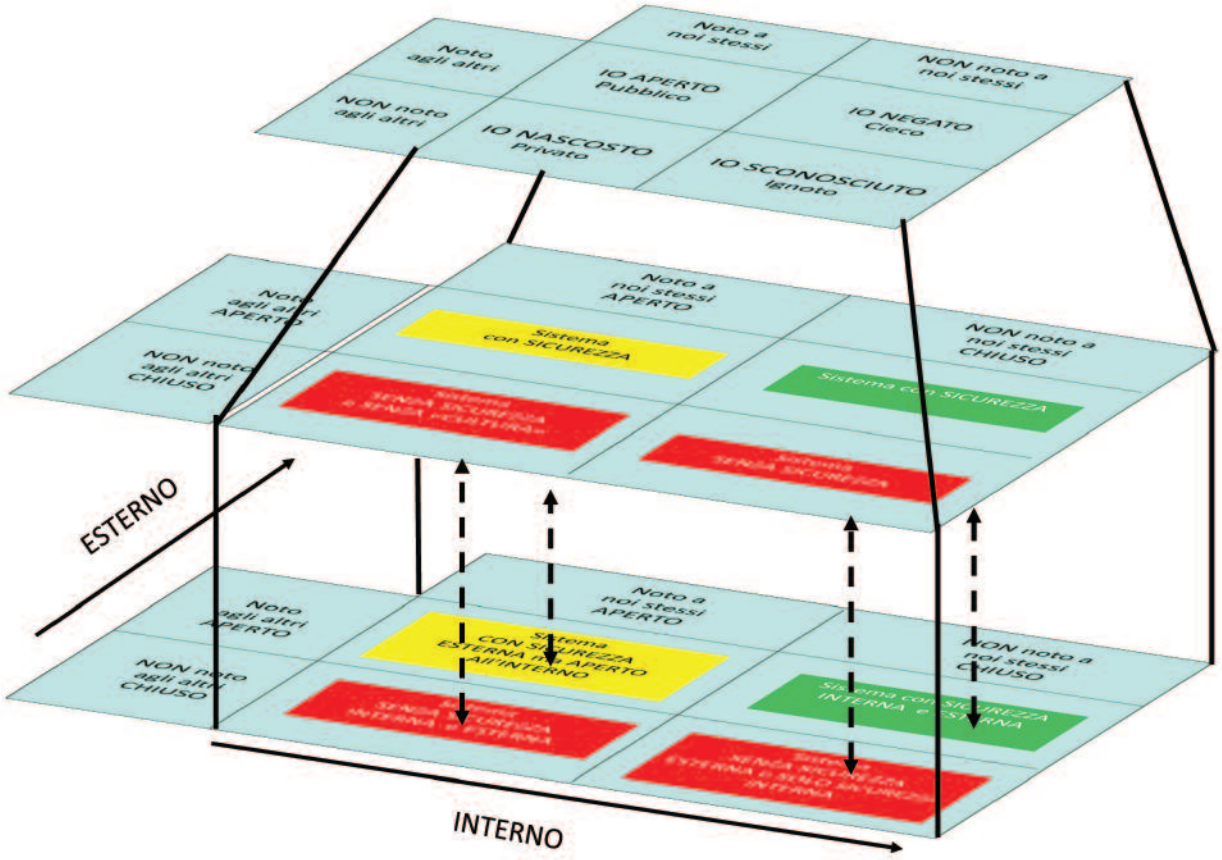
sure porta all'identificazione di quattro aree descritte di seguito, dove per informazioni si intendono a 360 gradi: personalità, conoscenze, emozioni e capacità.
Il primo quadrante, chiamato "Arena", rappresenta le informazioni che sono note sia al soggetto che agli altri. In questo senso è anche definita come area pubblica.
Il secondo quadrante, chiamato la "Facciata", comprende le informazioni che la persona conosce di sé ma che gli altri non sanno: è anche detta area privata.
Nel terzo quadrante, chiamato "Punto Cieco", le informazioni sulla persona sono note agli altri, ma non alla persona stessa. L'unico modo che la persona ha per acquisire informazioni in questa area cieca è attraverso il feedback diretto degli altri (espressamente richiesto o meno).
Il quarto quadrante è chiamato "Ignoto". Rappresenta le informazioni sconosciute sia al soggetto che agli altri. Non c'è modo di acquisire direttamente le informazioni contenute in questo quadrante, definito anche come area dell'inconscio.



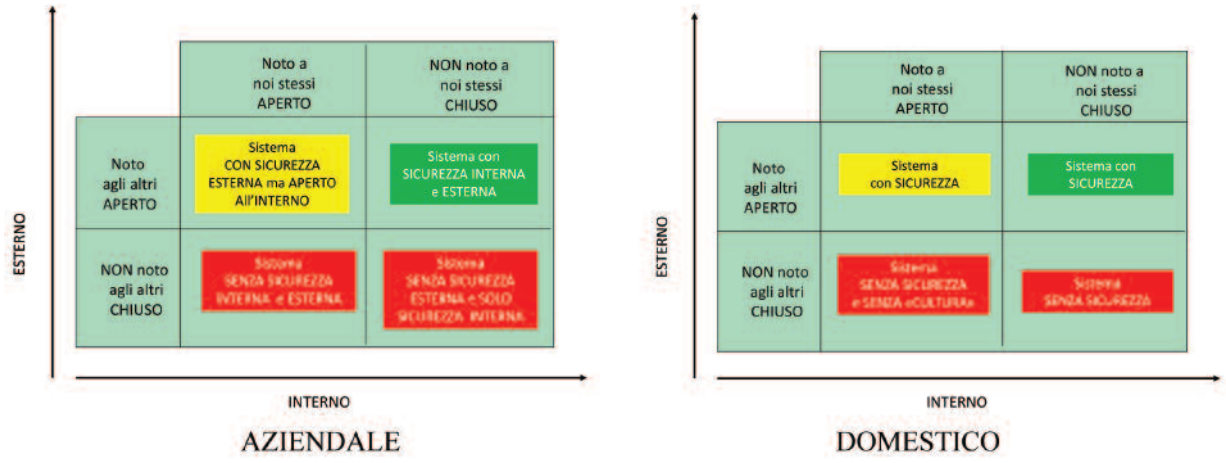
STEFANO GORLA

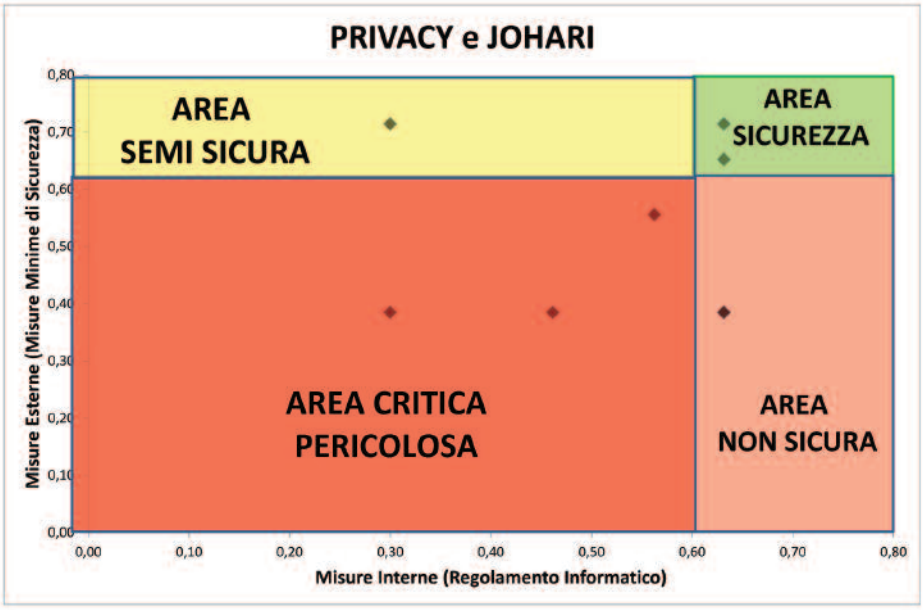
Privacy Business Unit Director - Digital Preservation Officer Consultant Seen Solution SRL e delegato regionale Lombardia Andip

Le informazioni che diamo all'esterno o che dall'esterno ci provengono possiamo associarle al trattamento del Dato Personale. Quanto siamo consapevoli della diffusione delle nostre informazioni? Quanto e cosa vogliamo condividere?
Facciamo una trasposizione tra le informazioni che la Finestra di Johari rappresenta e le informazioni che circolano o vengono trattate all'interno delle organizzazioni, ma non limitiamoci solo all'interno ma estendiamo al ragionamento anche verso i Social Network.
Dalla finestra di Johari possiamo individuare quali dati vogliamo condividere. Oggi non siamo più nell'era della tutela del dato personale (quando oramai è in rete il dato come viene gestito?), ma siamo nell'era del controllo dei dati personali. Ovvero siamo noi che con un preciso controllo, decidiamo quali dati mettere a disposizione.
Possiamo mappare questi aspetti in maniera sintetica come nella figura seguente (la Casa di Johari).
Partendo dal layer più basso (privato o aziendale dove convivono o dovrebbero convivere i controlli e le sicurezze logiche sia interne che esterne) migriamo verso l'alto sul secondo layer che possiamo definire "personale" cioè lo strato relativo a quanto noi comunichiamo i nostri dati personali e alle sicurezze utilizzate all'interno delle mura domestiche e non. Il tetto è la finestra di Johari originale che riguarda l'aspetto della comunicazione interpersonale.



Riportiamo il dettaglio del primo e secondo layer.





Abbiamo quindi due aspetti, una faccia della medaglia, dedicata al trattamento del dato personale all'interno delle organizzazione e l'altra faccia dedicata ai nostri dati personali ed a quanto vogliamo diffondere. Da una parte esiste il Titolare del trattamento e il dlgs 196/03 con i provvedimenti dell'Autorità, dall'altra ci siamo noi e solo noi che dobbiamo aumentare la nostra consapevolezza e controllo.

Se volessimo riportare su un grafico le sicurezze interne ed esterne otterremmo una figura di questo tipo. Guardando il grafico sono immediate alcune considerazioni.

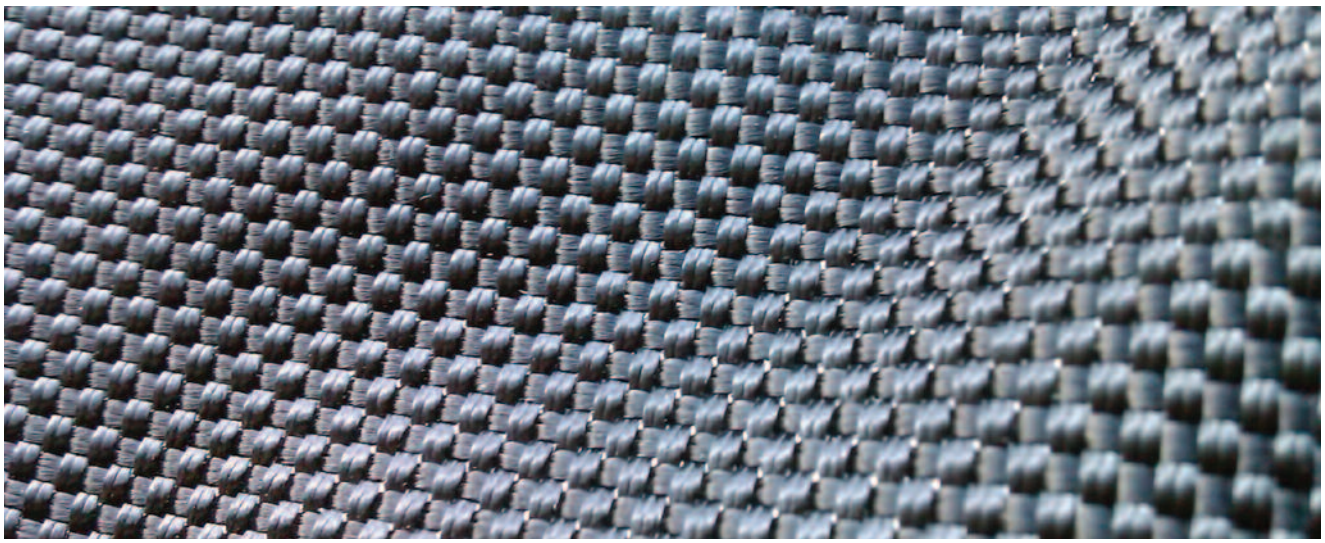
Nel caso ci siamo solo elevate misure di sicurezza interne posso bloccare e/o rallentare l'attività ma presto il fianco ad attacchi esterni, viceversa se ho solo elevate sicurezze esterne posseggo delle alte mura di difesa ma gli attacchi possono pervenire dall'interno.

In un ottica di tutela aziendale e di Cliente la posizione migliore è quella di garantire le sicurezze interne ed esterne (area verde) con un mix dedicato. Nulla di nuovo è sempre il rispetto della conformità in merito al Dlgs. 196/03, ma non sempre risulta così evidente la necessità del rispetto del c.d. Codice.

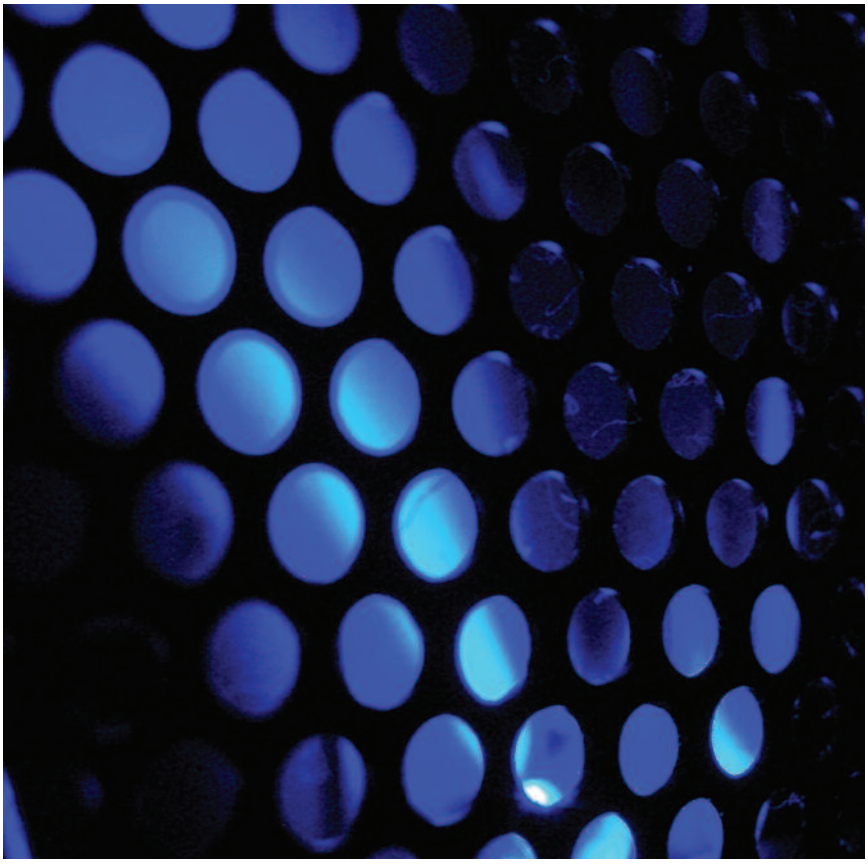
Se ci spostiamo sul secondo livello possiamo individuare attraverso un modello più semplice che non analizzi alcuni aspetti, ad esempio la perdita di immagine, e proiettare i risultati sulla mappa. Infatti come sono sicuri i nostri pc domestici e la nostra rete? Abbiamo conoscenza della sicurezza dei siti che visitiamo o delle operazioni che facciamo in rete?

Anche in questo caso il Garante è attento e sensibile al problema (compreso il Cyberbullismo) diffondendo in rete linee guida dedicate.

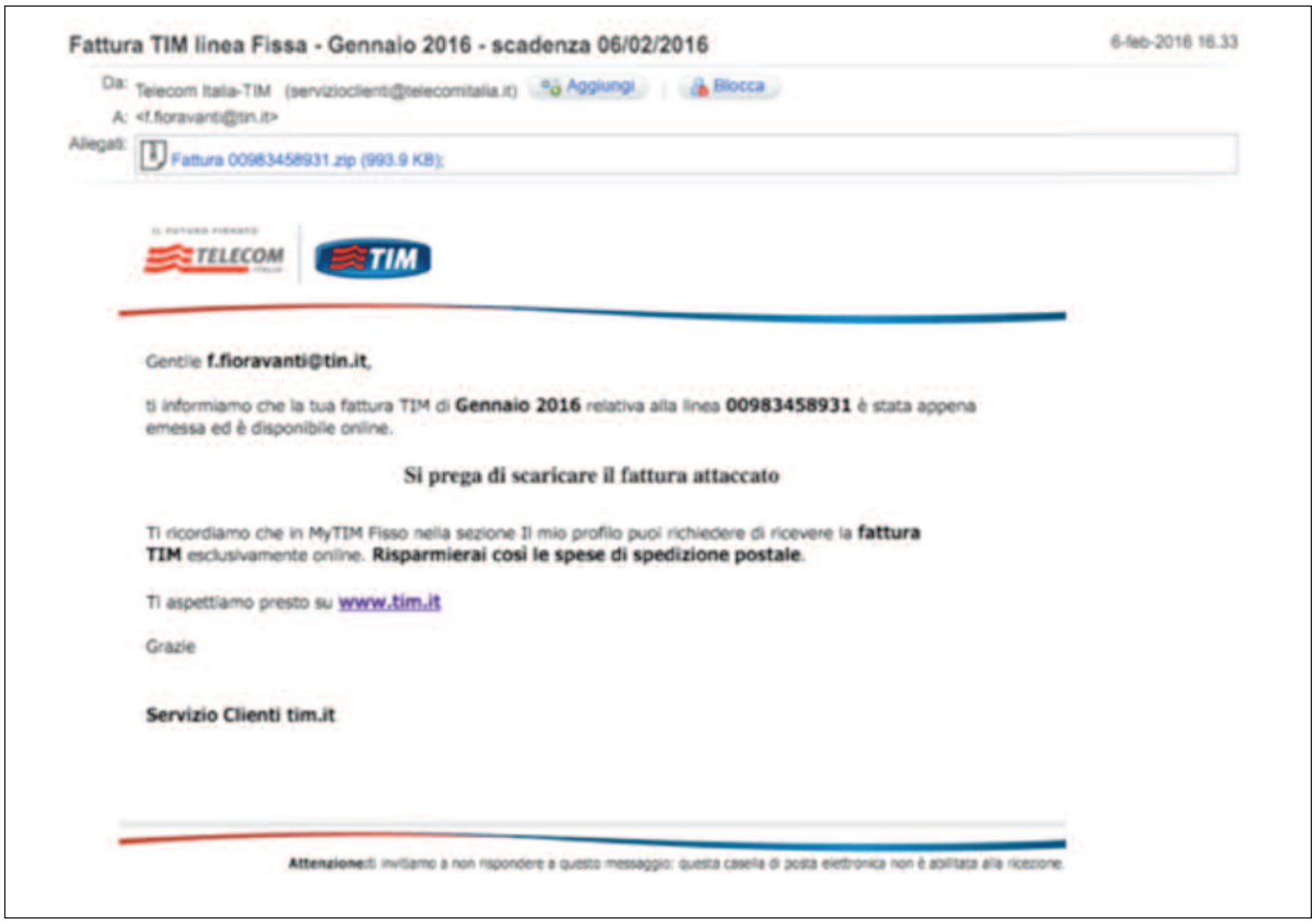
Il tetto della casa riguarda l'aspetto della comunicazione interpersonale che in un modo digitale assume connotazioni e caratteristiche. Possiamo comunicare nascondendoci dietro a falsi nickname o comunicare cose non vere (nessuno ci vede) ma questo aspetto riguarda più la scienza della psicologia e l'attività di controllo delle autorità preposte. ■



I cryptolocker



I giornali e le riviste sono pieni ultimamente del termine "cryptolocker" che già nel nome manifesta il proprio principio di funzionamento che consiste nel bloccare (lock), tramite un'azione di cifratura (crypto), i contenuti di un computer. L'aspetto inquietante è la richiesta di un riscatto per permettere all'utente di rientrare in possesso dei dati.
Questo tipo di attacchi rientra nel più generale gruppo dei ransomware (neologismo formato dai termini inglese ransom=riscatto e ware abbreviazione di software) che si propongono appunto di chiedere un riscatto a fronte di un'azione di ripristino di accesso al computer, ai suoi contenuti, etc.
Nonostante il 2015 abbia portato all'attenzione di tutti questo fenomeno, esso non è nuovo ed è tornato ad essere molto diffuso già dal 2013 anche se le origini risalgono al lontano 1989. Nel tempo, infatti, questi ransomware sono evoluti in complessità soprattutto riguardo alla possibilità di utilizzare chiavi di cifratura sempre più complesse che rendono in sostanza inefficace ogni tentativo di recupero dei dati.
Per difendersi è essenziale sia ca-



Fattura TIM linea Fissa - Gennaio 2016 - scadenza 06/02/2016

6-feb-2016 16.33

Da: Telecom Italia-TIM (servizioclienti@telecomitalia.it) Aggiungi Blocca

A: <f.fioravanti@tin.it>

Allegati: Fattura 00983458931.zip (993.9 KB);

TELECOM TIM

Gentile **f.fioravanti@tin.it**,

ti informiamo che la tua fattura TIM di **Gennaio 2016** relativa alla linea **00983458931** è stata appena emessa ed è disponibile online.

Si prega di scaricare il fattura attaccato

Ti ricordiamo che in MyTIM Fisso nella sezione Il mio profilo puoi richiedere di ricevere la **fattura TIM** esclusivamente online. **Risparmierai così le spese di spedizione postale**.

Ti aspettiamo presto su www.tim.it

Grazie

Servizio Clienti tim.it

Attenzioneti invitiamo a non rispondere a questo messaggio: questa casella di posta elettronica non è abilitata alla ricezione.

Fabrizio Fioravanti dopo la Laurea in Ingegneria Elettronica e l'abilitazione alla professione di Ingegnere consegue il Dottorato di Ricerca in Ingegneria Informatica e delle Telecomunicazioni titoli che gli permettono di operare come consulente prima e come quadro in aziende del settore ICT e della Sicurezza successivamente; nel 2008 approda come IT Manager a POLIMODA nel 2008 dove ancora lavora nello stesso ruolo. Ha al suo attivo pubblicazioni in conferenze e journal nazionali ed internazionali così come contributi a libri nonché un libro sulle metodologie di gestione dei progetti software.

pire come funzionino e come si diffondano questo tipo di attacchi, sia sapere quali precauzioni prendere per prevenire i danni oltre ovviamente a cosa fare in caso di infezione.

I cryptolocker come la maggior parte dei tentativi di phishing, variante del termine inglese fishing (letteralmente "pescare"), utilizza tecniche di ingegneria sociale per convincerci a compiere un'azione (scaricare ed aprire un allegato email, immettere le credenziali del nostro home banking, fornire i dati della carta di credito ad esempio) che poi si rivela essere una truffa. In passato l'ingegneria sociale passava attraverso il telefono con il quale un fantomatico tecnico chiedeva urgentemente le credenziali per scongiurare un danno aziendale enorme che magari l'interlocutore aveva non intenzionalmente causato usando frasi tipo "mi dia la sua password per controllare che non ci siano virus sulla posta"; oggi in genere tutte queste truffe sono legate a messaggi email che hanno un aspetto rassicurante per le persone (provengono da fonti ritenute affidabili, hanno formati, colori e logo riconoscibili) che quindi abbassano le difese e non prestano la dovuta attenzione al vero contenuto che molto

FABRIZIO FIORAVANTI

COME CONTRASTARE IL FENOMENO

Fare attenzione ai dettagli delle email

Ogni volta che riceviamo un'email per quanto innocua o sicura ci possa sembrare, non dobbiamo far calare il livello di attenzione. Controlliamo il mittente per vedere se è quello che dichiara di essere, verifichiamo che non ci siano errori di grammatica, ortografia o termini che sembrano essere usciti da un traduttore automatico perché sono un chiaro indice di falsificazione, controllare senza fare click tutti i link della mail e verificare che puntino davvero alla pagina che dichiarano, non aprire mai gli allegati ma al limite copiarli sul computer verificando che l'estensione del file sia quella che vi aspettate (se il file si presenza come un pdf ed ha estensione .js o .exe sicuramente è un ottimo candidato ad essere un falso) e se non siete sicuri della fonte contattate il mittente per verificare se vi ha inviato davvero quell'allegato; nel caso di enti o gestori che dichiarano di inviarvi documenti collegatevi al loro sito web e scaricate gli eventuali documenti solo da quella fonte. Considerate inoltre che i gestori con cui avete un contratto conoscono il vostro nome e cognome e quindi lo riporteranno nell'email, mentre le false email in genere riportano solo il vostro indirizzo email o un estratto del vostro indirizzo email: chi vi conosce vi chiama per nome non "per email".

Usare utenti non amministratori

In tutti i sistemi operativi, gli utenti possono essere di 2 tipi: limitati o amministratori. Il sistema operativo alla creazione di un utente vi chiede sempre se volete che sia limitato o amministratore: scegliete limitato per l'utente di uso quotidiano e create un amministratore per le operazioni di installazione o simili che effettuate solo sporadicamente. Gli utenti limitati non hanno accesso in modifica a tutte le cartelle di sistema e ai profili presenti sullo stesso computer degli altri utenti. Per questo motivo l'utente che utilizzate normalmente dovrà essere di tipo limitato perché se fosse amministratore, i danni del cryptolocker potrebbero essere ancora più estesi [giusto consiglio in generale, ma in realtà la maggior parte dei ransomware acquisisce i privilegi di admin] Ho volutamente semplificato, ma acquisiscono poteri di admin solo quelli che sfruttano exploit noti del SO ospite, in genere (come ho verificato in moltissimi casi) non sono in grado di lavorare come admin.

Accesso controllato ai dati in cloud

Accedete ai dati in cloud tramite le app specifiche per farlo o via web, non usate le utility che vi semplificano la vita mappando, ad esempio, come disco E: il vostro spazio su google drive o altro provider, perché questo sicuramente semplifica per voi l'accesso a quei dati, ma dobbiamo tenere conto che semplifica anche al cryptolocker l'accesso agli stessi dati.

Tenere un backup "fuori linea"

Sicuramente la prima regola per difendersi da qualunque tipo di attacco o danno ai dati contenuti nel computer consiste nell'avere un backup dei dati stessi e cioè una copia di sicurezza dei dati. Se teniamo questo backup ad esempio su un disco USB sempre connesso al computer, esso non sarà al sicuro dal cryptolocker, infatti, se l'utente può scrivere su quel disco, lo potrà fare anche il cryptolocker. Avere un backup "fuori linea" significa quindi tenerlo in un posto normalmente non accessibile al nostro utente: disco USB che stacchiamo alla fine del backup e riponiamo altrove, spazio in cloud cui accediamo solo via app o browser e salvataggi effettuati da software specifici che archiviano la copia di sicurezza in spazi per i quali il nostro utente non ha permessi di modifica.

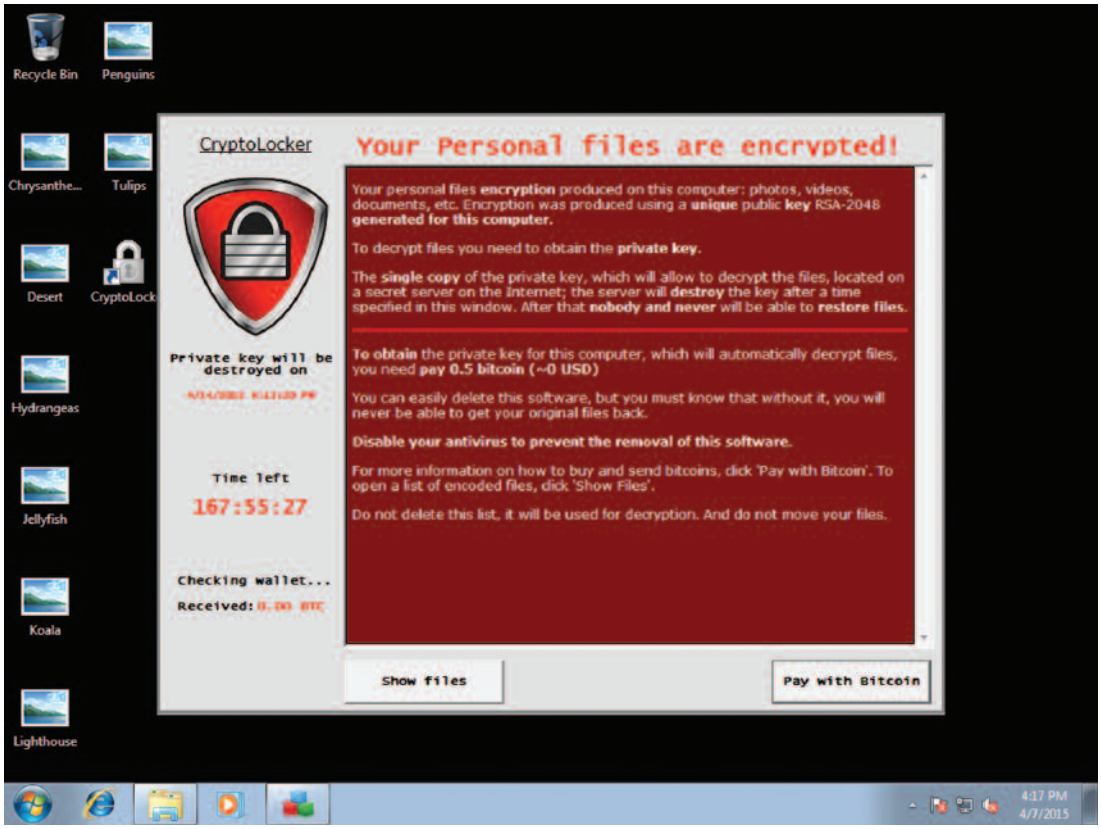
spesso contiene errori o segnali che se opportunamente analizzati avrebbero evitato di cadere nella truffa.
Ad inizio 2016 le caselle email di molti di noi sono state inondate, ad esempio, da false fatture Telecom (io personalmente ne ho ricevute moltissime a cui si sono aggiunte quelle di equitalia, di sda o di altri mittenti più o meno sconosciuti) in cui ci invitano a scaricare una presunta fattura contenuta in un file .zip allegato.
Purtroppo questo zip porta ad una infezione da cryptolocker. In questo caso era facile accorgersi della truffa in quanto il logo di Telecom

COME LIMITARE I DANNI SE SIAMO STATI ATTACCATI

Supponendo di non voler pagare il riscatto, cosa è bene fare per limitare i danni causati?
Dando per scontato che i file cifrati ormai sono persi, si tratta solo di limitare i danni. Come prima cosa staccare il computer dalla rete e spengerne la rete wireless, in modo da non avere connessioni attive con altri computer nelle vicinanze, poi spengere immediatamente il computer, fotografando magari lo schermo per avere memoria del cryptolocker che ci ha attaccato.
A questo punto se siete dei tecnici potete procedere in autonomia, altrimenti contattate un tecnico che possa aiutarvi ad eliminare il cryptolocker.
Nel caso vogliate operare da soli, la prima cosa da fare è di riavviare il computer in "modalità provvisoria" che non manda in esecuzione il file infetto. La modalità provvisoria più sicura è quella senza rete e senza interfaccia grafica, ma tutte le modalità sono corrette.
Da un altro computer potete scaricare uno dei tool che fanno pulizia del cryptolocker (avere fotografato lo schermo vi aiuta nell'identificare il tool che elimina la vostra infezione), anche se in genere i file del cryptolocker sono nella cartella temporanea dell'utente ed in esecuzione automatica ed una volta eliminati fermeranno il propagarsi dell'infezione a nuovi documenti.
Una volta fermato il cryptolocker dobbiamo fare i conti con i danni che ha provocato. Se abbiamo un backup dei soli dati o anche di tutto il computer precedente all'infezione, possiamo ripartire ripristinando quello che abbiamo salvato, altrimenti possiamo sperare di recuperare le copie di sicurezza dei file conservate ad esempio nelle cosiddette "shadow copy" di windows che se abilitate in maniera opportuna permettono tramite tool gratuiti scaricabili dalla rete di ripristinare i file da esse.
A questo punto possiamo copiare i file criptati (hanno tutti la stessa estensione, e possiamo quindi individuarli facilmente con una ricerca) su un disco esterno per non perdere la speranza di trovare un tool che li recuperi in futuro, ma ad oggi non ci sono risposte certe ed affidabili al problema.
Se il vostro utente era amministratore e il cryptolocker ha attaccato anche le cartelle di sistema, e non avete un backup completo da ripristinare la cosa migliore è forse quella di salvarsi tutti i dati e riportare il computer alla configurazione di fabbrica per ripulirlo da eventuali malfunzionamenti. (Consiglierei in ogni caso di ripristinare il sistema da zero).

era quello vecchio, il numero telefonico era errato ed al posto dell'usuale immagine di un bottone rosso rettangolare era presente un link oppure un testo contenente errori (tipo "il fattura attaccato"), senza contare il fatto che Telecom si rivolge a me come "Gentile Fabrizio Fioravanti" e non come "Gentile f.fioravanti@tin.it" . I segnali per evitare di cadere nella truffa quindi c'erano tutti, ma il testo quasi usuale, il formato della mail e il logo riconoscibile hanno tratto in inganno moltissime persone che ignorando tali segnali, si sono quindi fidate di un contenuto apparentemente innocuo: questa è appunto la frontiera attuale dell'ingegneria sociale in cui si presenta in un contesto apparentemente noto e tranquillizzante un elemento truffaldino che sfugge alla nostra attenzione perché spesso non curiamo con la necessaria attenzione i dettagli.

Analizziamo come opera un cryptolocker, semplificandone i passaggi, con l'aiuto della seguente immagine in cui è stata rappresentata la falsa email inviata sul nostro computer contenente un allegato che in genere non è il cryptolocker, ma un downloader (un programma apparentemente innocuo che scarica il cryptolocker stesso) che una volta scaricato manda in esecuzione il vero e proprio cryptolocker che invia a un



server sulla rete la richiesta di generazione di una coppia di chiavi di cifratura in cui la chiave pubblica viene consegnata al cryptolocker, mente la chiave privata rimane al sicuro sul server degli sviluppatori del cryptolocker.
Il sistema forte di cifratura a chiave pubblica/privata prevede, infatti, che con la chiave pubblica chiunque possa cifrare (e quindi rendere non accessibile) un file, ma solo chi ha la chiave privata riesce a decifrare il contenuto. Il meccanismo è lo stesso utilizzato ad esempio da alcuni programmi di posta elettronica per cifrare i messaggi email (sistema GPG ad esempio).
Una volta ottenuta la chiave pubblica, il cryptolocker comincia a cifrare file (in genere immagini, documenti, musica) cui l'utente collegato al computer ha accesso su tutti i dischi mappati sul computer. Questo significa che non solo andrà a colpire i documenti sul profilo dell'utente e sul disco C:, ma tutti i documenti sui dischi cui l'utente ha accesso in modifica. Se quindi ad esempio avete connesso un disco USB anch'esso sarà oggetto di attacco, così come in una rete aziendale saranno a rischio tutte le unità su server di rete mappate per il vostro utente. Il problema potenzialmente potrebbe non fermarsi alle unità disco del computer o a quelle della rete locale, ma se avete installato sul computer una delle utility che vi presenta un disco in cloud (sia esso google drive, dropbox, o altro) come un'unità disco del computer anche i documenti ivi contenuti saranno oggetto di attacco.
Per assicurarsi che il malcapitato utente si accorga di cosa sta accadendo il desktop è rimpiazzato con una immagine su cui compare la chiave pubblica ed una richiesta di pagamento che può essere in valuta (euro, dollari, ad esempio) o in bitcoin; il Bitcoin è una moneta digitale che può essere posseduta e trasferita ad altri in maniera pseudo-anonima; la natura virtuale della moneta, l'assenza di organi preposti al suo controllo e l'architettura della rete atta a sostenerne le transazioni impediscono il blocco della sua circolazione nonché limitano di molto le possibilità della svalutazione visto che l'immissione di valuta è controllata e stabilità a priori con una formula dipendente dal tempo, rendendola appetibile oltre che una serie assolutamente lecita di operazioni anche per operazioni che hanno bisogno di essere occultate. Anche se il riscatto può sembrare a volte piccolo per chi non conosce la valuta virtuale (1 bitcoin ad esempio) dobbiamo ricrederci valutando il fatto che attualmente il valore del bitcoin è di circa 350€.

Quello che lascia letteralmente a bocca aperta leggendo uno dei rapporti di Symantec (Symantec Website Threat Report Part-1 2015) sono i numeri riguardanti i ransomware in genere e più in particolare quelli dei crypto-ransomware. Secondo tale rapporto, infatti, fra il 2013 e il 2014 siamo passati da 4.1 milioni di attacchi a 8.8 milioni di attacchi di tipo ransomware duplicando quindi il numero di attacchi rispetto al precedente anno.
L'esplosione dei crypto-ransomware è invece ancora più strabiliante essendo passati dai circa 8000 del 2013 agli oltre 370.000 del 2014 con un incremento approssimativo di 45 volte.
L'esplosione nei numeri è probabilmente proporzionale all'aumento del guadagno da parte di queste cybergang che bloccando i documenti per noi importanti (documenti e fatture aziendali) o a noi cari (immagini, video e documenti personali) fanno leva sulla necessità da parte nostra di voler entrare di nuovo in possesso del materiale cui non possiamo più accedere.
La realtà dei fatti, con il maggior numero di cryptolocker moderni, è che risulta impossibile recuperare i propri dati senza avere la chiave privata conservata sul server remoto che è in mano alla cybergang. I tentativi a forza bruta hanno scarsa probabilità di successo o richiedono dei tempi enormi su un computer tradizionale.
In assenza di contromisure preventive (backup fuori linea, salvataggi in cloud, shadow copy, etc) l'unica possibilità per tentare di recuperare i documenti sembra proprio essere quella di pagare, cosa che molti hanno fatto in questi ultimi anni fornendo così ai criminali informatici dietro queste azioni nuovi fondi per sviluppare ulteriori tecniche di attacco sempre più sofisticate.
Il pagamento purtroppo non garantisce di rientrare in possesso dei nostri documenti poiché i server su cui sono conservate le coppie di chiavi cambiano velocemente, talvolta vengono bloccati dagli investigatori rendendo impossibile l'accesso alla tanta agognata chiave privata.
Inoltre chi ci garantisce che dopo un'azione di tipo criminale quale bloccare i nostri documenti si abbia a che fare con una controparte che mantiene la parola data?
Molto spesso, infatti, ci esponiamo a rischi ancora maggiori pagando e se anche si decide di farlo (cosa che sconsiglio) è necessario adottare delle misure particolari quali ad esempio quelle di usare una carta di credito "usa e getta" che il sistema bancario offre, oppure di comprare i bitcoin sulle piattaforme di trading ufficiali invece di seguire i link del cryptolocker, per poi trasferire i bitcoin all'indirizzo che ci hanno comunicato. ■

Il Report McAfee Labs rileva come solo il 42% dei professionisti della sicurezza si affida a informazioni di intelligence sulle minacce condivise

Un'indagine condotta su 500 professionisti della sicurezza valuta l'adozione e il valore percepito della condivisione dell'intelligence sulle minacce nella sicurezza informatica in azienda; nuovi picchi di ransomware del 26% nel quarto trimestre 2015

- *Solo il 42% dei professionisti di sicurezza informatica intervistati dichiara di utilizzare informazioni condivise sulle minacce informatiche*
- *Gli intervistati percepiscono che i maggiori ostacoli alla condivisione dell'intelligence sulle minacce informatiche sono le policy aziendali (54%), le normative di settore (24%) e la mancanza di informazioni su come potrebbero essere utilizzate (24%)*
- *McAfee Labs ha registrato una crescita di nuove minacce ransomware del 26% nel quarto trimestre 2015*
- *Nel quarto trimestre 2015 i ricercatori hanno osservato un aumento del 72% di nuovi campioni di malware mobile trimestre su trimestre*

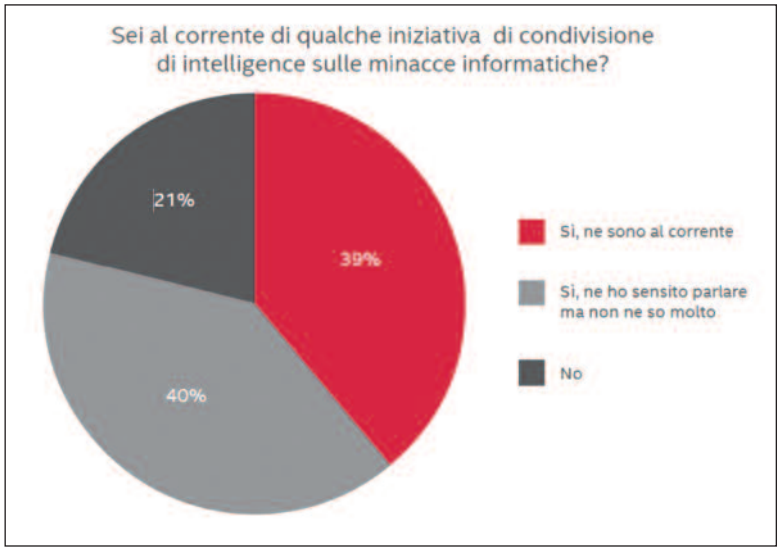
Intel Security ha rilasciato il Report sulle minacce McAfee Labs: marzo 2016, che valuta gli atteggiamenti di 500 professionisti di sicurezza informatica a proposito della condivisione dell'intelligence delle minacce informatiche (CTI-Cyber Threat Intelligence), esamina il funzionamento interno del RAT (tool di amministrazione remota) Adwind e registra picchi di ransomware, malware mobile, oltre a fornire una panoramica sulla situazione complessiva del malware nel quarto trimestre del 2015.

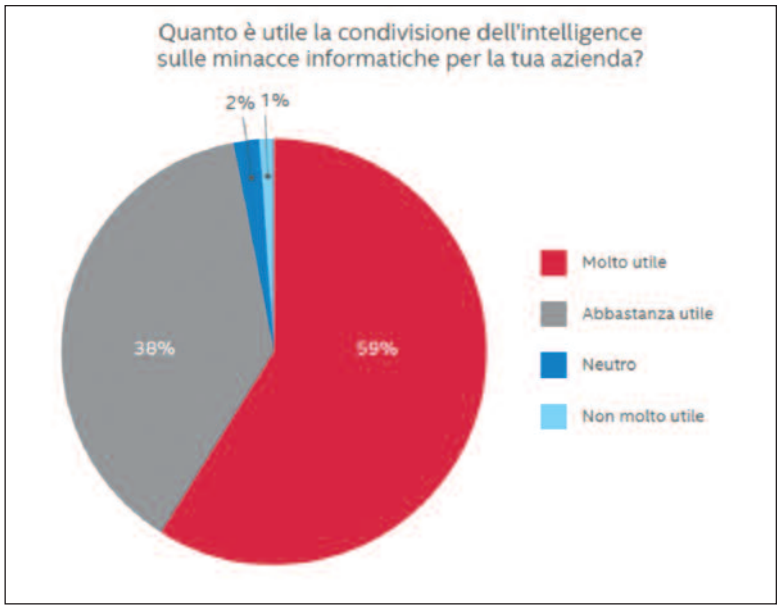
Nel 2015, Intel Security ha effettuato un sondaggio che ha coinvolto 500 professionisti della sicurezza operanti in una vasta gamma di settori in Nord America, Asia-Pacifico e in Europa per valutare la consapevolezza relativamente alla condivisione di intelligence sulle minacce (CTI), il valore percepito di queste attività per la sicurezza aziendale, e quali fattori possono ostacolare una sua maggiore implementazione nelle strategie di sicurezza. Gli intervistati hanno fornito un quadro prezioso della situazione e sulle potenziali opportunità dall'introduzione della CTI nelle aziende:

- **Valore percepito e adozione**. Del 42% degli intervistati che hanno dichiarato di fare ricorso alla condivisione di intelligence sulle minacce, il 97% ritiene che consenta loro di fornire una migliore protezione alla propria azienda. Il 59% giudica che la condivisione sia "molto preziosa" per la propria azienda, mentre il 38% la considera "abbastanza di valore."
- **Intelligence specifica per settore.** Un quasi unanime 91% di intervistati si è dichiarato interessato all'intelligence sulle minacce informatiche specifica per settore, con il 54% che si è detto "molto interessato" e il 37% "in qualche modo interessato." Settori come quelli dei servizi finanziari e delle infrastrutture critiche potrebbero beneficiare maggiormente di un approccio alla CTI per settori verticali, data la natura altamente specializzata delle minacce che McAfee Labs ha rilevato indirizzate a questi due settori di importanza fondamentale.

- **Disponibilità a condividere.** Il 63% degli intervistati si è espresso positivamente circa la possibilità di andare al di là della sola ricezione di dati di CTI e di voler contribuire realmente mettendo a disposizione i propri dati, a patto che siano condivisi all'interno di una piattaforma sicura e privata. Tuttavia, l'idea di condividere le proprie informazioni è vista in modo differente, con il 24% per cui è "molto probabile" mentre per il 39% rimane "piuttosto probabile".
- **Tipi di dati da condividere.** Alla domanda su quali tipi di informazioni sulle minacce sarebbero disposti a condividere, gli intervistati hanno fatto riferimento a dati relativi al comportamento del malware (72%), seguiti dalla reputazione di URL (58%), reputazione di indirizzi IP esterni (54%), reputazione di certificati (43%) e reputazione di file (37%).
- **Ostacoli alla diffusione della CTI**. Quando è stato chiesto il motivo per cui non hanno attuato politiche di CTI nelle loro imprese, il 54% degli intervistati ha identificato nelle policy aziendali una delle ragioni principali, seguita dalle normative di settore (24%). Il resto degli intervistati le cui aziende non condividono report di dati si sono detti interessati, ma hanno bisogno di maggiori informazioni (24%), o esprimono perplessità sul fatto che i dati possano essere ricondotti alla società o a loro stessi come individui (21%). Questi risultati evidenziano una mancanza di esperienza, o di conoscenza delle varietà di opzioni di integrazione di CTI oggi disponibili, oltre a una scarsa conoscenza delle implicazioni legali della condivisione di CTI.

"Data la determinazione dimostrata dai criminali informatici, la condivisione di CTI diventerà uno strumento importante per spostare l'ago della bilancia della sicurezza informatica dalla parte di coloro che si fanno carico della protezione", ha dichiarato Vincent Weafer, vice presidente del gruppo McAfee Labs di Intel Security. "Ma la nostra indagine suggerisce che per affermarsi la CTI deve superare le barriere delle policy organizzative, le restrizioni normative, i rischi associati con la fiducia e la poca conoscenza dello strumento, prima che il suo potenziale possa essere pienamente realizzato".



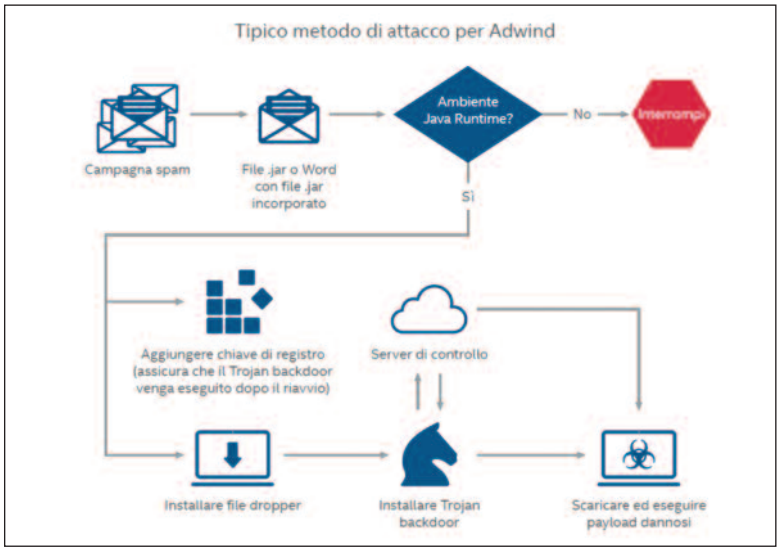


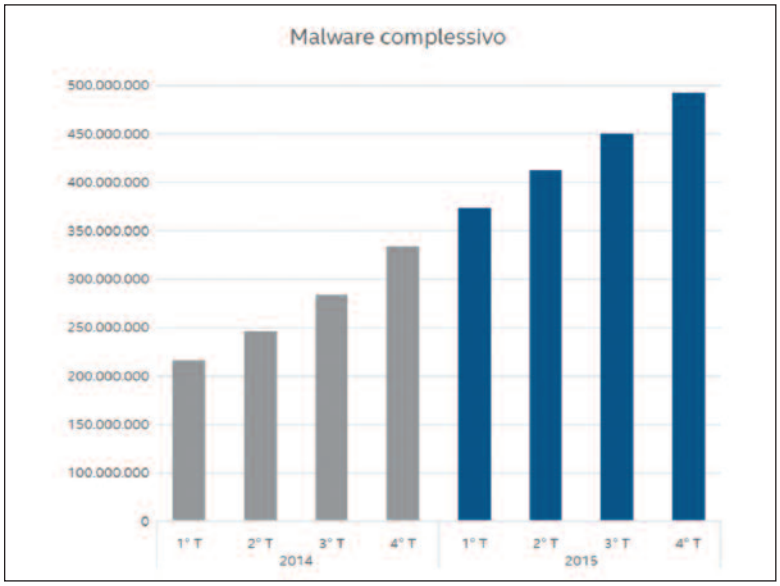
Il report di questo trimestre prende in esame anche il funzionamento del RAT (Remote Administration Tool) Adwind, un Trojan backdoor basato su Java in grado di colpire varie piattaforme che supportano Java. Adwind, tipicamente, si propaga attraverso campagne di email spam con allegati carichi di malware, pagine web compromesse e download guidati. Il report McAfee Labs il-

lustra un rapido aumento del numero di campioni di file .jar identificati dai ricercatori di McAfee Labs come Adwind, pari a 7.295 nel quarto trimestre 2015, con un balzo del 426% rispetto ai 1.388 registrati nel primo trimestre del 2015.

Attività generale delle minacce:

- **Il ransomware accelera di nuovo**. Dopo il leggero rallentamento registrato a metà anno, il ransomware è tornato a crescere rapidamente, con un aumento trimestre su trimestre del 26% nel quarto trimestre 2015. Il codice ransomware open source e il ransomware-as-a-service continuano a semplificare la diffusione degli attacchi, le campagne Teslacrypt e CryptoWall 3 continuano ad ampliare la loro portata, e le campagne ransomware continuano ad essere economicamente redditizie. Un'analisi effettuata in ottobre 2015 relativamente al ransomware CryptoWall 3 s è addentrata nelle opportunità finanziarie di tali campagne, e i ricercatori di McAfee Labs hanno rilevato come da una singola campagna sono stati movimentati 325 milioni di dollari di pagamenti di riscatto da parte delle vittime.
- **Il malware mobile torna a salire**. Il quarto trimestre del 2015 ha visto un aumento del 72% trimestre su trimestre di nuovi campioni di malware mobile, da cui si evince come gli autori di malware stiano compilando nuovi malware più velocemente.
- **Il Rootkit crolla**. Il numero di nuovi campioni di malware rootkit è sceso precipitosamente nel quarto trimestre, proseguendo una tendenza già evidenziata per questo tipo di attacchi. McAfee Labs attribuisce una parte di questo declino, che ha avuto inizio nel terzo trimestre 2011, all'adozione di processori Intel® a 64 bit e di Microsoft Windows a 64 bit. Si tratta di tecnologie che includono funzionalità di sicurezza come Kernel Patch Protection e Secure Boot, che insieme contribuiscono a una migliore protezione contro minacce di tipo rootkit malware.
- **Alti e bassi del malware in generale**. Dopo tre trimestri di calo, nel quarto trimestre, il numero totale di nuovi campioni di malware ha ripreso la sua ascesa, con 42 milioni di nuovi codici dannosi scoperti, il 10% in più rispetto al trimestre precedente e il secondo valore più elevato mai registrato da McAfee Labs. In parte, la crescita nel quarto trimestre è stata trainata da 2,3 milioni di nuovi campioni di malware mobile, pari a 1 milione in più rispetto al terzo trimestre.





- **Declino dei file firmati binari dannosi.** Il numero di nuovi file binari dannosi firmati è sceso ogni trimestre nel corso del 2015, fino a raggiungere nel quarto trimestre il livello più basso dal secondo trimestre 2013. McAfee Labs ritiene che il calo può essere attribuito in parte al fatto che i vecchi certificati diffusi in modo significativo nel mercato nero o sono in scadenza o sono stati revocati man mano che le aziende migrano verso funzioni di hashing più forti. Inoltre, le tecnologie come Smart Screen (parte di Microsoft Internet Explorer ma adottata anche in altre sezioni di Windows) rappresentano ulteriori strumenti di fiducia che potrebbero rendere la firma di codici binari dannosi meno vantaggiosa per gli autori di malware.

Una copia completa Report sulle minacce McAfee Labs: marzo 2016 e per ulteriori informazioni sugli argomenti trattati e sul panorama delle minacce del quarto trimestre 2015, è disponibile all'indirizzo http://www.mcafee.com/March2015ThreatsReport.

Per un elenco di suggerimenti per la sicurezza e di indicazioni su come aziende e singoli utenti possono proteggersi dalle minacce evidenziate in questo report trimestrale, si prega di visitare i siti: **Enterprise Blog** e **Consumer Safety Tips Blog**.

"Se la stessa indagine venisse fatta in Italia probabilmente la percentuale dei professionisti di sicurezza informatica che dichiara di utilizzare informazioni condivise sulle minacce informatiche sarebbe inferiore, perché nel nostro paese non esiste ancora una corretta sensibilizzazione in merito" afferma Davide Baldinotti, General Manager della Unit J.Soft di Computer Gross "di conseguenza le persone tendono ad essere scettiche e a non avere fiducia nella condivisione e comunicazione dei dati, considerandole una minaccia anziché un'opportunità. Tuttavia noi siamo molto positivi" – continua Baldinotti – "in pochi anni abbiamo già avuto ottimi risultati insieme agli operatori di canale che hanno deciso di puntare su questo trend di mercato. Attraverso un grande lavoro di sensibilizzazione del nostro Team qualificato, aggiornato e specializzato, i partner hanno dimostrato sempre più interesse e proattività su tutti gli aspetti della Security. Attraverso un portafoglio di offerta integrato e complementare, oltre al valore intrinseco delle soluzioni Intel, stiamo lavorando per diffondere maggior conoscenza e consapevolezza sulle numerose opzioni di integrazione di Cyber Threat Intelligence che oggi sono disponibili. Ci sono tutte le basi per essere confidenti di riuscire a contribuire a veicolare non solo l'importanza, ma anche l'urgenza della condivisione e della comunicazione dei dati e delle informazioni".

La nostra indagine suggerisce che per affermarsi la condivisione di Intelligence delle minacce deve superare alcune barriere, tra cui le policy aziendali e la poca conoscenza dello strumento," ha dichiarato **Ferdinando Torazzi, Regional Director di Italia e Grecia, Intel Security**. *"Alcuni di questi ostacoli cominciano a cadere e, parallelamente, l'uso delle CTI diverrà un componente essenziale delle difese di un'azienda, perché i dati strutturati e arricchiti consentono di rispondere più rapidamente e con una visione migliore sugli eventi attuali e di prevedere gli eventi futuri."* ■

COMPUTER GROSS

www.computergross.it

intel Security

www.mcafee.com

Kaspersky Lab scopre problemi di sicurezza nei sistemi smart di monitoraggio del traffico

Nel tentativo di studiare i problemi di sicurezza delle infrastrutture di trasporto delle smart city e offrire suggerimenti su come affrontarli, un esperto del Global Research & Analysis Team (GReAT) di Kaspersky Lab ha condotto una ricerca sul campo su alcuni sensori stradali che raccolgono informazioni sul flusso del traffico cittadino. Di conseguenza, Kaspersrsky Lab ha scoperto che i dati raccolti e processati dai sensori possono essere sensibilmente compromessi. Ciò potrebbe influenzare le decisioni future delle autorità cittadine sullo sviluppo delle infrastrutture stradali.

Le infrastrutture di trasporto delle moderne megalopoli rappresentano un sistema molto complesso, che comprende diversi generi di sensori del traffico e stradali, telecamere e persino semafori intelligenti. Tutte le informazioni raccolte da questi dispositivi vengono trasferite e analizzate in tempo reale dalle autorità dedicate. Le decisioni sulle future costruzioni stradali e sulla pianificazione delle infrastrutture di trasporto possono basarsi su queste informazioni. Se i dati vengono compromessi, possono comportare per la città una perdita di milioni di dollari.

In particolare, se qualcuno ottenesse acceso fraudolento alle infrastrutture di trasporto, potrebbe accadere quanto segue:

- I dati ottenuti dai sensori stradali potrebbero venire compromessi nel tentativo di sabotarli o di rivenderli a terze parti;
- Modifica, falsificazione o persino eliminazione di informazioni critiche;
- Demolizione dell'equipaggiamento esistente;
- Sabotaggio del funzionamento dei servizi dell'autorità cittadina.

Un esperto di Kaspersky Lab ha recentemente condotto a Mosca una ricerca su una rete di sensori stradali che raccolgono informazioni sul flusso del traffico – in particolare sul numero di veicoli che transitano, il loro tipo e la velocità media. Queste informazioni vengono trasferite al centro di comando dell'autorità cittadina. Le autorità incaricate del controllo del traffico ricevono le informazioni e le utilizzano per supportare e aggiornare una mappa del traffico stradale in tempo reale. La mappa, in cambio, può servire come fonte di informazioni per la costruzione di un sistema stradale cittadino o persino per automatizzare il controllo dei semafori.

Il primo problema di sicurezza scoperto dal ricercatore è il nome del vendor chiaramente impresso sulla scatola del sensore. Questa informazione fondamentale ha aiutato il ricercatore di Kaspersky Lab a scoprire online ulteriori informazioni su come opera il dispositivo, che software utilizza, e così via. Il ricercatore ha scoperto che il software utilizzato per interagire con il sensore, così come la documentazione tecnica, erano disponibili sul sito del vendor. Infatti, la documentazione tecnica spiegava molto chiaramente che comandi potessero essere inviati da terze parti al dispositivo.

Semplicemente camminando vicino al dispositivo, il ricercatore è stato in grado di accedervi via Bluetooth, in quanto non era stato implementato alcun processo di autenticazione affidabile. Chiunque, con un dispositivo abilitato Bluetooth e un software che usa il metodo forza bruta per scoprire le password con diverse varianti, può connettersi a un sensore stradale in questo modo. Ma cosa fare in seguito?

Usando il software e la documentazione

tecnica, il ricercatore è stato in grado di osservare tutti I dati raccolti dal dispositivo. Ha inoltre potuto modificare il modo in cui il dispositivo raccoglie nuove informazioni: ad esempio cambiando il tipo di veicolo registrato da macchina a camion o cambiando la velocità media del traffico. Di conseguenza, tutte le nuove informazioni raccolte erano false e non applicabili in risposta ai bisogni della città.

"Senza le informazioni raccolte da questi sensori, l'analisi del traffico in tempo reale e i conseguenti adeguamenti del sistema di trasporto cittadino non sarebbero possibili. Questi sensori possono essere usati in futuro per realizzare un sistema di semafori intelligenti e per decidere che genere di strade dovrebbero essere costruite e come il traffico dovrebbe essere organizzato, o riorganizzato, in determinate aree della città. Tutte queste problematiche implicano che il funzionamento dei sensori e la qualità dei dati raccolti dovrebbero essere accurati e stabili. La nostra ricerca ha illustrato quanto sia semplice compromettere questi dati. È fondamentale affrontare ora queste minacce perché in futuro potrebbero interessare una parte maggiore delle infrastrutture delle città", ha commentato **Denis Legezo, Security Researcher del Global Research and Analysis Team (GReAT) di Kaspersky Lab**.

Kaspersky Lab consiglia di applicare alcune misure per aiutare a impedire un attacco informatico condotto con successo contro i dispositivi dell'infrastruttura di trasporto. Esse includono:

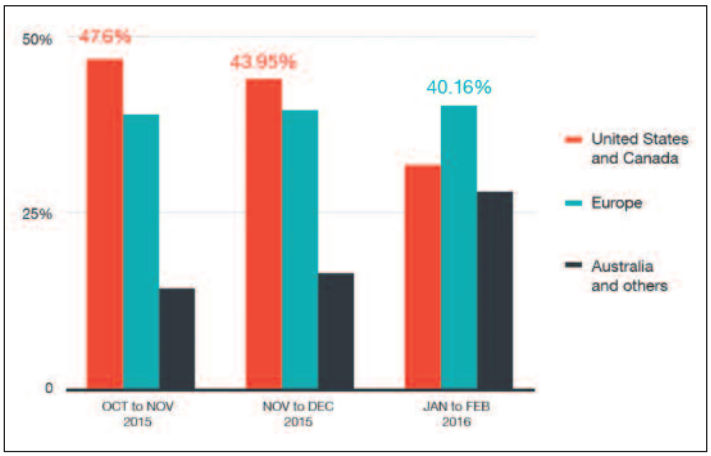
- Rimuovere o nascondere il nome del vendor sul dispositivo, in quanto esso può aiutare un criminale a trovare gli strumenti per accedere al dispositivo;
- Cambiare i nomi di default del dispositivo e celare gli indirizzi MAC del vendor quando possibile;
- Usare due livelli di autenticazione sui dispositivi con connessione Bluetooth e proteggerli con password forti;
- Cooperare con i ricercatori di sicurezza per scoprire e risolvere le vulnerabilità.

Per avere ulteriori informazioni sulla sicurezza del settore dei trasporti, è possibile leggere il blogpost su **Securelist.it**

La ricerca è stata condotta in relazione con il supporto offerto da Kaspersky Lab all'iniziativa Securing Smart Cities. Per ulteriori informazioni sui problemi di sicurezza informatica attuali e futuri delle smart city e su come risolverli, visitare ***Securing Smart Cities***. ■

La "truffa del CEO" arriva anche in Europa

I criminali fingono di essere il CEO dell'azienda per muovere i soldi aziendali



Anche l'FBI ha pubblicato un **alert** sul drammatico aumento delle truffe **Business Email Compromise**, capaci di frodare aziende in tutto il mondo per un valore di 2,3 miliardi di dollari. Ora i laboratori Trend Micro, leader globale nella sicurezza per il cloud, certificano il loro incremento in Europa. Queste truffe non discriminano gli obiettivi e colpiscono ogni tipo di azienda indipendentemente dalla sua grandezza. L'ultima a colpire in maniera più rapida e massiccia è la frode che è stata denominata "**La truffa del CEO**", che vede i truffatori identificarsi con dirigenti di alto livello. L'obiettivo di questa frode è entrare in possesso dell'account email di una figura executive dell'azienda per deviare somme di denaro a conti fraudolenti.

Facendo finta nella maggior parte dei casi di essere il CEO dell'azienda, i criminali sono in grado di spostare i soldi aziendali attraverso richieste di trasferimento di denaro ad altri membri dell'azienda. L'attacco utilizza tecniche di ingegneria sociale, nel momento in cui i truffatori hanno bisogno di ottenere l'indirizzo email del dirigente.

I laboratori Trend Micro avvisano che le operazioni di monitoraggio de "La truffa del CEO" hanno rilevato una crescita degli attacchi diretti alle aziende europee dall'inizio del 2016, in contemporanea con una diminuzione dell'interesse per gli obiettivi in USA e Canada.

Questo tipo di truffa ricorda lo spear phishing, con la differenza che il malware è opzionale o addirittura assente. Il cyber criminale tenta di creare un messaggio email il più credibile e familiare per ridurre al minimo i sospetti nel destinatario.

Le soluzioni Trend Micro sono in grado di proteggere le aziende di tutte le dimensioni da attacchi di questo tipo, attraverso la tecnologia di **Social Engineering Attack Protection**.

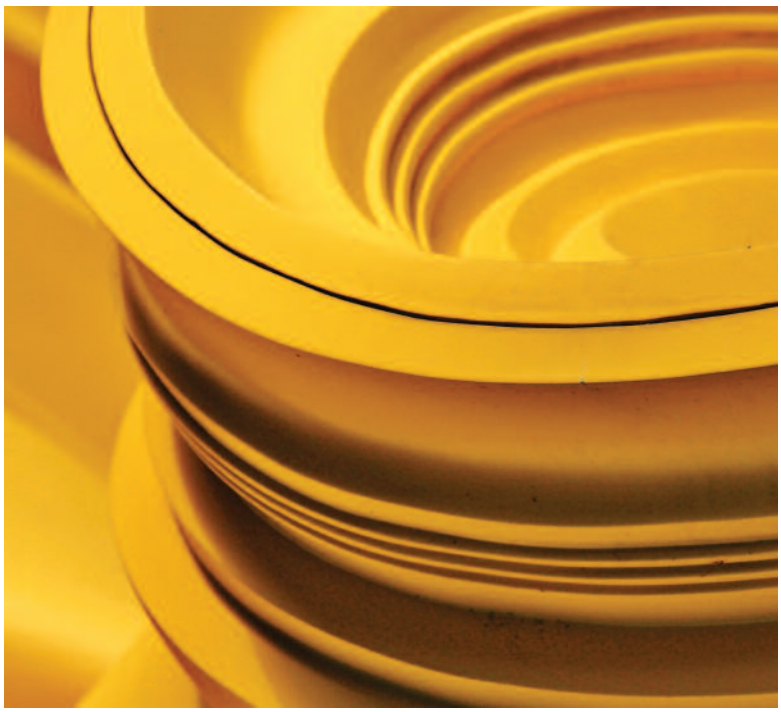
Questa tecnologia è integrata nelle soluzioni InterScan Messaging Security e Hosted Email Security e fornisce un ulteriore livello di protezione attraverso il controllo delle intestazioni delle email, delle tattiche di social engineering, dei comportamenti contraffatti e il rilevamento di malware correlati alle truffe.

Queste soluzioni sono fornite attraverso le capacità di sicurezza email ed endpoint della **Trend Micro Smart Protection Suites** e **Network Defense**. ■

Via libera del Parlamento UE, la privacy europea diventa realtà

Voto finale del Parlamento UE che ha portato oggi a compimento un percorso durato più di 4 anni per l'emanazione di nuove regole sulla protezione dei dati personali. Maggiori diritti per i cittadini per creare la fiducia necessaria per l'economia digitale in Europa. Multe fino a 20 milioni di euro o al 4% del fatturato annuo per i trasgressori. Previsione della figura di un responsabile per vigilare sull'effettivo rispetto delle regole. Bernardi: "Come nel caso dei privacy officer anglosassoni, ruolo cruciale anche per implementare business senza infrangere le regole"

Giornata storica per l'UE con l'approvazione definitiva del nuovo Regolamento Privacy, che aiuterà i cittadini a recuperare il controllo dei propri dati personali e a creare un livello di protezione elevato ed uniforme in tutti gli Stati membri dell'Unione Europea per un pieno sviluppo dell'economia digitale.
Con il voto finale del Parlamento Europeo, avvenuto a Strasburgo durante la seduta plenaria di oggi, termina così un percorso durato più di quattro anni, in cui è stata operata una completa revisione della normativa UE sulla protezione dei dati, per sostituire una direttiva targata "CE" che risaliva al lontano 1995, quando internet era ancora agli albori.
Il nuovo Regolamento, che in Italia prenderà il posto dell'attuale Codice della Privacy (Dlgs 196/2003), è stato concepito per dare ai cittadini un maggiore controllo sulle proprie informazioni personali in un mondo ormai digitalizzato da smartphone, social media, internet banking e trasferimenti globali.
"Questo è un grande successo per il Parlamento UE e un fiero 'sì' ai diritti dei consumatori e alla libera concorrenza nell'era digitale - ha affermato Jan Philipp Albrecht nel comunicato ufficiale della UE - I cittadini saranno in grado di decidere loro stessi quali dati personali vogliono o no condividere. Il nuovo regolamento, fornirà anche chiarezza per le imprese attraverso la definizione di una singola legge in tutta l'UE, creando fiducia, certezza del diritto, e una concorrenza più equa".
Le norme emanate oggi, prevedono nuove disposizioni sul diritto all'oblio, sul consenso chiaro ed informato al trattamento dei dati personali, sul diritto di trasferire i dati



ad un altro fornitore di servizi, e quello di essere informati quando i propri dati sono stati violati, ma anche sull'obbligo per le imprese di utilizzare un linguaggio chiaro e comprensibile nelle informative sulla privacy, con multe che potranno arrivare fino a 20 milioni di euro o al 4% del fatturato annuo dei trasgressori.

"Con il Regolamento approvato oggi, l'UE detta nuove e più stringenti regole che non devono essere recepite come un peso da parte delle imprese, perché in realtà è stato finalmente dato ordine per un mercato digitale finora dominato indiscriminatamente dai colossi del web americani, che ora dovranno invece rimboccarsi le maniche per allinearsi - ha commentato Nicola Bernardi, presidente di Federprivacy - Un'altra nota positiva, è la previsione della figura di un **responsabile** della protezione dei dati, che avrà il compito di vigilare che la propria azienda rispetti effettivamente le regole, fungendo da punto di contatto sia con gli interessati che con l'Autorità Garante. Ma questo ruolo sarà cruciale anche perché, come avviene nel caso dei privacy officer nei paesi anglosassoni, questa figura potrà fornire consulenza al management per utilizzare correttamente i dati personali per implementare le proprie attività di business senza però infrangere le regole."

Il regolamento sarà pubblicato a breve nella Gazzetta ufficiale dell'Unione Europea, ed entrerà in vigore 20 giorni dopo. Le nuove disposizioni saranno direttamente applicabili in tutti gli Stati membri due anni dopo tale data. ■

ICT FORUM Security®

CONOSCERE E PREVENIRE LE NUOVE MINACCE INFORMATICHE

17° Edizione

19 OTTOBRE 2016
ROMA

HOTEL ROMA AURELIA ANTICA
Via degli Aldobrandeschi, 223

AGGIORNAMENTI SUL SITO
WWW.TECNAEDITRICE.COM


TIM Impresa Semplice
Cosa aspetti? Con Mail Power
puoi condividere tutte le idee che hai in testa.
Comunica con i tuoi clienti in tempo reale. Vai su Nuvola Store e scopri il nuovo servizio Mail Power.
I tuoi clienti sono aggiornati su tutte le tue novità tramite email, SMS e Social Network e tu puoi monitorare il successo di ogni tua iniziativa.
TIM
Per maggiori informazioni sui servizi
vai su nuvolastore.it
Promuovi
il tuo business