Cybersecurity Trends

Edizione italiana, N. 4 / 2018

INTERVISTE VIP:

Luciano FLORIDI
Antonella VIOLA
Vittorino ANDREOLI

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Central Folder: eHealth

Global Cyber Security

La Fondazione GCSEC è un'organizzazione senza scopo di lucro, creata per promuovere la sicurezza informatica in Italia e nel resto del mondo. Il Centro, fondato e finanziato da Poste Italiane, ha sede a Roma e collabora con Istituzioni Italiane e Internazionali Governative, enti privati, istituti di ricerca e organismi internazionali.
La missione della Fondazione è quella di sviluppare e diffondere la conoscenza e la consapevolezza sulla sicurezza informatica, creando le condizioni per migliorare le capacità, le competenze, la cooperazione e la comunicazione tra i diversi attori coinvolti nell'uso e nella protezione di Internet.

Information Sharing
Creazione di modelli di information sharing pubblico - privato

Threat Intelligence
Analisi di modelli di attacco e delle tecnologie necessarie a velocizzare l'analisi stessa

Sensibilizzazione
Campagne di sensibilizzazione multi-livello

Formazione
Attività di formazione e corsi di specializzazione e master

Fondazione Global Cyber Security Center
Viale Europa, 175 – 00144 Roma
www.gcsec.org

GLOBAL CYBER SECURITY CENTER

Indice

Investimenti nazionali e cyber readiness

Autore: Nicola Sotira

L'Unione Europea, da tempo, sta adottando una serie di misure allo scopo di aumentare la sua resilienza e la preparazione nel settore della sicurezza informatica. Già nel 2013, ha definito una serie di obiettivi e azioni volte a ridurre la criminalità informatica e sviluppare, inoltre, una maggiore capacità di autodifesa indirizzando le industrie verso una politica coerente di sviluppo del settore IT. La direttiva NIS, emanata nel 2016 dall'Unione Europea, è il primo tassello fondamentale che promuove una cultura della gestione dei rischi. La Direttiva introduce, infatti, requisiti di sicurezza obbligatori per i principali operatori economici e in particolare per tutti gli operatori appartenenti alle infrastrutture critiche. Nel frattempo, gli attacchi informatici sono in aumento e ogni volta che gli impatti sono significativi, viene sollecitato l'intervento da parte del legislatore attraverso l'emanazione di nuove leggi e regolamenti.

Queste richieste sono dovute alla trasformazione della società di oggi, che sta diventando sempre più dipendente dal digitale, e ai danni su larga scala che possono essere causati dagli attacchi informatici.

In questo scenario, l'intervento legislativo dovrebbe considerare anche l'impatto dei costi monetari che la società è disposta a sostenere, oltre a comprendere il livello della minaccia.

La valutazione dei costi, da parte del legislatore, servirà a capire dove questi potranno essere assorbiti, se dai consumatori attraverso l'aumento dei prezzi, dal legislatore o dalle aziende produttrici.

Sempre su questo tema gli investimenti nazionali, come la difesa, sono difficili da valutare in modo puramente obiettivo. Inoltre, occorre tenere presente che gli investimenti nella sicurezza IT sono ricorrenti. Prodotti e software sono come gli edifici, hanno un costo iniziale di progettazione e un costo di manutenzione e aggiornamento.

Sicurezza e usabilità andranno poi sempre più di pari passo; sino ad oggi i sistemi di sicurezza hanno sempre influenzato l'esperienza dell'utente. Basti pensare come ancora oggi il tema dell'autenticazione in molte applicazioni richieda iterazioni che limitano di molto la flessibilità e spesso non sono proponibili in ambienti mobile. Nello scenario digitale l'usabilità e la semplicità saranno fattori chiave per il successo, il nuovo business digitale non può accettare limitazioni della flessibilità dell'utente. Questo scenario richiede spesso una nuova progettazione dei sistemi e delle infrastrutture a supporto del digitale, un altro spunto per il legislatore su come guidare la trasformazione digitale del Paese.

Un tema degno di nota è inoltre quello della dissuasione, che è particolarmente complessa nel dominio del cyberspazio rispetto al mondo fisico. La deterrenza dipende dal poter attribuire atti a persone o Istituzioni e quindi la possibilità di punire i colpevoli.

Nell'attuale scenario digitale, l'attribuzione di attacchi informatici sulla rete è complessa, le fonti possono essere falsificate o riscritte lungo il percorso. L'attribuzione, molto spesso, richiede un'analisi molto costosa. Punire gli attaccanti può quindi essere problematico se lavorano al di fuori della giurisdizione del governo. Siamo pronti per una discussione che coinvolga investimenti pubblici e privati per supportare la sicurezza IT a tutto tondo? Possiamo quantificare, tenendo conto dei vari aspetti, il valore da investire a livello nazionale? Credo che oggi sia giunto il momento di avviare un dialogo nazionale che inserisca questo tema nella logica degli investimenti del Paese e che coinvolga in questo processo le aziende e gli operatori del settore ... ■

BIO

Nicola Sotira è Direttore Generale della Fondazione Global Cyber Security Center GCSEC e Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

Autore: **Marco Obiso,**

Coordinatore per la cyber security, International Telecommunications Union, Ginevra

Nell'anno che ha visto celebrare il primo decennio del programma mondiale *„Child Online Protection"*, vorremmo sottolineare il lavoro di GCSEC, editore della versione italiana di Cybersecurity Trends; grazie alla Fondazione, sono state tradotte in italiano e promosse non solo le ultimissime versioni delle linee guida sulla *Child Online Protection* (COP), ma anche la mostra *"Eroi e Vittime dei Social Media, dai geroglifici a Facebook"*, patrocinata dall'ITU, che da due anni è itinerante nella penisola grazie all'impegno di Poste Italiane.

Questo stesso anno ha anche visto la nascita della prima edizione di *"Cybersecurity Mediterranean"* (Noto, 10-11 Maggio) – lanciato dalla Swiss Webacademy, dove la responsabile di COP in ITU, Carla Licciardello, ha interagito con i bambini delle Scuole Medie durante il tradizionale *"awareness day"*. Il "sistema" di eventi internazionali PPP preceduti dall'*awareness day* per bambini e adulti, ha raggiunto quindi 3 congressi macro-regionali (con sedi in Romania, Svizzera e Italia), supportati da partner istituzionali di 8 paesi, tra i quali GCSEC.

Viene anche offerta, con puntuale regolarità, la rivista online trimestrale Cybersecurity Trends, tradotta in 4 lingue e adattata ai specifici contesti nazionali di Francia, Italia, Regno Unito, Romania e Moldavia.

PARIS CALL
FOR TRUST AND SECURITY IN CYBERSPACE
11 • 12 • 2018

Il lavoro di Swiss Webacademy, una delle prime entità a firmare la *"Paris Call for Trust and Cybersecurity in Cyberspace"*, durante il periodico evento Internet Governance Forum (IGF), conferma la volontà di condividere esperienze e fornire contributi di alto livello, al fine di aver una conoscenza più ampia sull'ecosistema nel quale viviamo.

Ci vuole molta volontà, molta energia, e tutta la generosità di un lavoro non-profit per raggiungere e consolidare questi obiettivi. E' un elemento che ci sembra doveroso evidenziare che proprio quest'anno c'è stato un calo di tali eventi a livello internazionale.

Con questo numero dedicato alla *eHealth*, editori e redattori della rivista portano alla vostra attenzione, con oggettività, punti di vista di ricercatori, specialisti, ed esperti E' da sottolineare quanto, dal medico al *"vendor"* tutti hanno una preoccupazione comune: la fragilità del sistema, soprattutto per quanto riguarda la parte del paziente, se l'insieme tecnologico e umano non sono perfettamente rodati. Ancora una volta, il nostro grado di cultura (continua) dei rischi digitali sarà l'elemento che darà alle prestazioni un valore aggiunto oppure una fonte di rischio maggiore.

AuspicandoVi, cari lettori, un 2019 pieno di salute, vi auguriamo una piacevole lettura. ■

Data protection di applicazioni mobili in ambito sanitario

Autore: Roberto Obialero

BIO

Esperto di sicurezza informatica, in possesso di una vasta esperienza in ruoli tecnici e di sviluppo del business maturata insieme ad aziende dell'offerta. Da 18 anni opera nel campo della sicurezza informatica occupandosi di progettazione di reti sicure, protezione delle informazioni, business continuity management, vulnerability assessment, analisi e gestione di incidenti informatici e computer forensics. Nel corso degli ultimi quattro anni ha intrapreso la carriera di advisor freelance avviando collaborazioni in ambito cybersecurity e data protection, analisi e gestione del rischio aziendale e formazione con importanti società di consulenza nei mercati PA, Finance, Retail ed Automotive.
E' in possesso delle certificazioni indipendenti GPPA e GCFA ottenute attraverso il programma SANS-GIAC americano e della certificazione ISO 27000 Lead Auditor. Perfezionato in "Computer Forensics & Data Protection" e "Data Protection & Data Governance" organizzati dal Dipartimento di Informatica Giuridica dell'Università Statale di Milano. Membro del Comitato Tecnico Scientifico Clusit collabora attivamente alla realizzazione di progetti di ricerca nell'ambito Cybersecurity & Data Protection con le principali community di settore; nel corso degli ultimi anni è stato speaker in occasione di diversi eventi di rilevanza nazionale, oltre ad aver collaborato alla redazione di diverse pubblicazioni ed articoli per conto di riviste specializzate.

Introduzione

L'utilizzo delle tecnologie mobili nell'ambito sanitario è un settore emergente e molto promettente della cosiddetta eHealth, ovvero il complesso delle risorse, soluzioni e tecnologie informatiche applicate alla salute ed alla sanità. La sanità mobile, per cui è stato coniato lo specifico termine mHealth è destinata a integrare i metodi tradizionali di erogazione delle cure sanitarie anche sotto il profilo di assistenza al malato.

La sfida attuale è muoversi in tale contesto affrontando le importanti questioni di sicurezza delle applicazioni, la corretta gestione dei dati sensibili e l'interoperabilità tra le soluzioni disponibili, considerando inoltre una ulteriore difficoltà ravvisabile nel fatto che attualmente la normativa applicabile a tali soluzioni è da assumersi per analogia e spesso si incontra un vuoto normativo per fattispecie direttamente correlabili a queste soluzioni.

Nell'articolo verranno caratterizzati i rischi e le opportunità derivanti dall'adozione di queste tecnologie ormai pervasive e di notevole potenziale innovativo.

Utilizzo di applicazioni e dispositivi mobile in ambito sanitario

L'utilizzo delle applicazioni informatiche fruibili attraverso i terminali mobili, tablet e smartphone, possono portare degli apprezzabili vantaggi sia nei confronti dei pazienti che nei confronti del personale medico; nei paragrafi successivi sono elencati alcuni dei principali casi d'uso che si avvalgono dell'ausilio delle nuove tecnologie.

Applicazioni informatiche mobile rivolte a operatori sanitari

La caratteristica comune di questo gruppo di applicazioni è quella di essere rivolte ad un numero ristretto e predefinito di operatori sanitari, i quali in funzione del loro ruolo chiave associato a precise responsabilità dovranno essere preventivamente registrati al servizio cui dovranno autenticarsi. Esempi delle funzionalità che possono permettere tali applicazioni sono:

1. **monitoraggio dei pazienti ed anamnesi in corsia:** è possibile tenere sotto controllo continuo alcuni parametri vitali dei pazienti e di conseguenza

supportare in modo più tempestivo e preciso le attività di diagnosi da parte del personale medico;

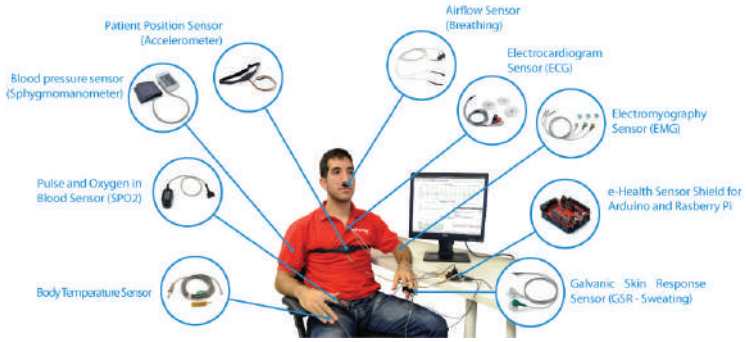
2. **somministrazione terapie:** è possibile fornire sul dispositivo mobile in dotazione al personale paramedico le informazioni sul corretto dosaggio dei medicinali da somministrare ai pazienti e mediante l'uso di tecnologie RFID comunicare in tempo reale alla Farmacia interna della Struttura Sanitaria le informazioni sull'effettivo utilizzo delle scorte;

3. **controllo dei referti:** le cartelle cliniche ed i referti degli esami sono consultabili attraverso i terminali mobili in dotazione al personale medico autorizzato al trattamento dei dati del paziente, secondo regole definite internamente per le Cartelle Cliniche e dalla normativa in ambito di Fascicolo Sanitario Elettronico per i referti;

4. **monitoraggio da remoto dei pazienti (teleassistenza):** in questo caso i dispositivi mobili permettono una evoluzione e semplificazione della strumentazione dedicata alla teleassistenza. Essendo dotati di sensori, saranno "indossati" dai pazienti e i valori misurati mediati da applicazioni di teleassistenza saranno resi disponibili al personale medico per le attività di diagnosi e di somministrazione delle cure; un altro aspetto importante di questa applicazione è rappresentato dal supporto erogabile al paziente da parte del personale adibito a servizi socio-assistenziali che consentirà il trattamento del decorso post patologia al di fuori delle strutture ospedaliere. Risulta fin da subito evidente che tale applicazione richiede delicatissime considerazioni sul fatto che tali dispositivi non siano certificati come dispositivi medicali e pertanto occorre fin da subito precisare che tali valori, saranno sempre considerati esclusivamente per il quadro anamnestico del paziente.

Applicazioni informatiche mobile rivolte ai pazienti

La caratteristica di questo gruppo di applicazioni fruibili in mobilità è quella di essere rivolta ad un pubblico potenzialmente molto vasto di utenti; trattando tali servizi dati sensibili si rende necessaria l'adozione di meccanismi in grado di assicurare la privacy del soggetto interessato (esempio: raccolta del consenso, gestione identità e rilascio di token di autenticazione, cifratura delle comunicazioni e dei dati, ecc…).



Esempi delle funzionalità che possono permettere tali applicazioni sono:

1. **prenotazione esami:** è possibile interagire, se in possesso delle credenziali di autenticazione con le infrastrutture di prenotazione esami attraverso i terminali mobili; questo comporta un risparmio sia nel tempo speso dal cittadino che da parte delle strutture sanitarie per l'evasione delle pratiche amministrative;

2. **ritiro referti:** gli esiti degli accertamenti diagnostici sono resi disponibili attraverso una piattaforma informatica a cui il cittadino può accedere previa autenticazione e nel rispetto delle linee guida e dei decreti in tema di referti online;

3. **ritiro cartelle cliniche elettroniche:** allo stesso modo il paziente potrà accedere tramite dispositivo fisso o mobile alle informazioni pertinenti il suo ricovero all'interno di una struttura ospedaliera compilate dal personale sanitario;

4. **controllo dei parametri vitali e terapie diabetologiche:** al paziente vengono forniti dei dispositivi mobili in grado di tenere sotto controllo alcuni parametri (ad esempio il valore della pressione sanguigna oppure il valore della glicemia); in funzione dei valori misurati, è possibile per il paziente seguire, sotto la sorveglianza medica, la terapia più appropriata;

5. **notifica di assunzione dei farmaci:** per i pazienti che hanno la necessità di prendere regolarmente farmaci in modo controllato esiste la possibilità di avere dei meccanismi in grado di ricordare l'esigenza. Tramite le applicazioni di telemedicina è possibile notificarne la corretta assunzione al personale assistenziale;

6. **app dedicate alla buona salute:** questo ambito in forte espansione indirizza prevalentemente un'esigenza dell'utenza finale a seguito del miglioramento nello stile di vita; nonostante il mercato generalmente non lo consideri, anche in questo caso si possono presentare problematiche di privacy e anche relative ad una possibile profilazione degli utenti dettata da esigenze di marketing dei fornitori dei servizi e dei prodotti.

L'introduzione nelle attività quotidiane del cittadino delle applicazioni per mobile sopra citate comporta indubbiamente una maggiore efficienza del sistema sanitario cui potranno associarsi risparmi potenzialmente considerevoli da parte della Pubblica Amministrazione.

Gestione dell'infrastruttura di erogazione dei servizi

L'infrastruttura elaborativa attraverso la quale vengono erogati i servizi informatici può essere gestita, in funzione delle politiche organizzative della Struttura Sanitaria, direttamente da un Servizio Informatico appartenente all'Azienda Sanitaria oppure può essere esternalizzata; nei paragrafi seguenti vengono presentati i profili di gestione della privacy ai sensi della normativa vigente.

Gestione diretta

Nel caso di gestione diretta la responsabilità dell'adozione delle misure idonee di sicurezza è totalmente in capo alla Azienda Sanitaria; per quanto concerne il Regolamento Europeo l'Azienda eserciterà le funzioni di Titolare del trattamento dei dati.

Affidamento in outsourcing

Nel caso di affidamento della gestione del servizio informatico in regime di outsourcing, a seconda del livello di servizio concordato, occorrerà negoziare accuratamente il contratto di servizio e definire con precisione l'assunzione delle responsabilità inerenti le garanzie di protezione della privacy e della sicurezza; in questo caso la Struttura Sanitaria manterrà la titolrità del trattamento dei dati e dovrà provvedere alla nomina del fornitore quale responsabile del trattamento.

Servizi erogati secondo paradigma cloud computing

Nel caso di ricorso a servizi erogati in modalità Cloud Computing occorrerà fare le debite distinzioni a seconda del modello di riferimento, cloud pubblico, ibrido o privato e dalla modalità di erogazione del servizio (IaaS, PaaS o SaaS) e, come nel caso precedente, definire con attenzione ruoli e responsabilità a garanzia di privacy e sicurezza negli accordi contrattuali di fornitura. Particolare rilevanza in questo caso, trattandosi di dati sensibili, è assunta dal luogo in cui verranno fisicamente trattati i dati, se dentro o fuori dai confini europei; anche in questo caso le figure di titolare e responsabile del trattamento risulteranno distinte tra Struttura Sanitaria e fornitore di servizi cloud.

Misure di sicurezza organizzative

Al fine di tutelare adeguatamente, tenendo conto delle peculiarità dei servizi offerti e della delicatezza dei dati trattati, gli aspetti legati alla privacy del cittadino ed al mantenimento di un livello accettabile di sicurezza

è importante affiancare alle misure di sicurezza di tipo tecnologico una serie di misure di tipo organizzativo che vengono di seguito descritte.

Mobile Security Policy

Nei casi visti precedentemente, di applicazioni per operatori sanitari, occorre presidiare il contesto mobile affiancando al documento principale relativo alle politiche generali di sicurezza una policy specifica applicabile alla fruizione in mobilità dei servizi informatici. In tale documento occorre che siano chiaramente definiti i ruoli e le responsabilità, i meccanismi di provisioning e gestione dei terminali mobili, i meccanismi di autenticazione, le regole di utilizzo, l'eventuale ammissibilità dell'utilizzo dei terminali personali (BYOD), un elenco esplicito di applicazioni fruibili in modalità mobile, le esigenze di protezione, le misure da attuare in caso di furto o smarrimento del terminale ecc.

Il ruolo di coordinamento del CISO e del DPO

Una corretta gestione degli aspetti legati alla sicurezza ed alla privacy non può prescindere dalla presenza di un opportuno ruolo di coordinamento delle attività: per quanto concerne la tematica della sicurezza tale ruolo è sotto la responsabilità del CISO (Chief Information Security Officer). Questa figura, idealmente alle dipendenze delle funzioni apicali della Struttura Sanitaria, sovrintende alla definizione ed all'applicazione delle politiche di sicurezza dell'organizzazione e provvede ad eseguire l'analisi dei rischi. E' il naturale interlocutore del CIO (Chief Information Officer) per quanto concerne l'implementazione delle misure di sicurezza mantenendo un giusto compromesso con l'efficacia dei sistemi informativi, le mutevoli esigenze di business e gli adempimenti normativi richiesti. Per quanto concerne gli aspetti legati alla privacy la figura di riferimento è il Data Protection Officer che, di concerto con l'Ufficio Legale dell'organizzazione, avrà il compito la consulenza ed il controllo delle attività descritte nei paragrafi successivi.

Classificazione dei dati personali in base alla tipologia

All'interno dei sistemi informativi moderni, caratterizzati da una crescente complessità e dispersione di risorse, è di fondamentale importanza provvedere alla classificazione dei dati, in termini di disponibilità integrità e riservatezza sulla base della loro appartenenza a dati personali o dati sensibili: questo in quanto le esigenze di protezione di un dato attraverso il quale sia possibile risalire alla patologia di un individuo sono sicuramente maggiori rispetto a quelle relative ad un dato di tipo amministrativo oppure tecnico. Risulta quindi critico per la Struttura Sanitaria l'adozione di un processo di classificazione ed aggiornamento periodico di tali dati anche ai fine dell'esecuzione periodica dell'analisi dei rischi.

Analisi e gestione dei rischi

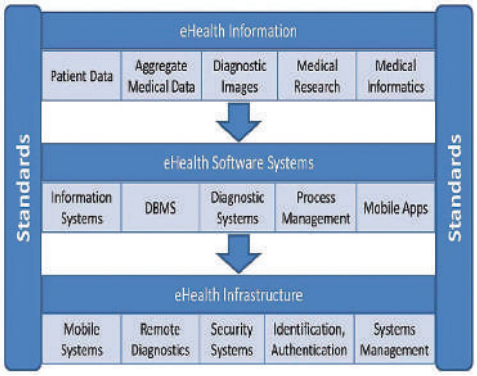
L'obiettivo principale dell'adozione delle misure di sicurezza è la mitigazione del rischio di natura informatica, ed in ottica GDPR rispetto ai diritti dei soggetti interessati. Queste informazioni vengono desunte attraverso l'esecuzione di un risk assessment che può essere di carattere generale, ovvero rappresentato dallo *standard* internazionale ISO 27001 relativo alla sicurezza delle informazioni, ISO29151 ai sensi della protezione dei dati personali sensibili oppure contestualizzata verso un settore specifico quale quello sanitario ed assicurativo americano denominato HIPAA.

Al termine dell'analisi del rischio risultano evidenti i settori in cui, rispetto alle *best practices* di settore, le misure di sicurezza risultano meno adeguate. Al termine di questa fase si ottiene una lista di prescrizioni applicabili e per ogni misura viene attribuito un budget di spesa; da qui si definisce un piano organico di interventi. Applicando la fase successiva denominata trattamento del rischio si pongono in essere gli interventi più urgenti, contraddistinti da un buon compromesso tra costo e mitigazione del rischio; tale attività viene ripetuta periodicamente all'interno del processo sino a giungere ad un livello di rischio definito accettabile.

Formazione del personale

Il personale che dovrà gestire ed utilizzare le applicazioni mobile dovrà ricevere l'opportuna formazione sia per quanto riguarda le regole sul trattamento dei dati personali che per quanto concerne i rischi di sicurezza e le modalità per mitigarli; è opportuno che le sessioni di formazione vengano ripetute periodicamente in caso di aggiornamenti significativi alle applicazioni oppure per sensibilizzare l'utenza verso l'introduzione di nuove minacce alla sicurezza.

Misure di sicurezza tecnologiche



Ad integrazione delle misure organizzative sopra citate occorre porre in essere delle misure tecnologiche a contrasto delle minacce informatiche che consentano di fronteggiare i rischi in modo organizzato e con un efficace dispendio di energie.

Infrastruttura di accesso ai servizi mobile e requisiti di sicurezza

Gli accessi in mobilità alle applicazioni possono avvenire principalmente in due modalità, ovvero attraverso la rete dei gestori di servizi mobile UMTS e successive declinazioni oppure attraverso una rete WI-FI che, data la particolare sensibilità dei dati trattati in ambito sanitario, è auspicabile che sia di tipo privato e resa disponibile solo dopo aver valutato accuratamente i rischi connessi ed applicato i criteri di sicurezza adeguati.

Per quanto concerne l'accesso alle reti pubbliche dei gestori delle telecomunicazioni non si possono ovviamente richiedere degli adeguamenti specifici, ma occorrerà fare in modo che le connessioni alle applicazioni che trattano dati sensibili avvengano almeno tramite canale cifrato, con algoritmo crittografico aggiornato, mediante mutua autenticazione tra utente e server applicativo.

Anche le connessioni locali alla rete WI-FI dovranno avvenire mediante una rete privata protetta da accessi esterni indesiderati in protocollo cifrato e con registrazione dei tentativi di accesso; la comunicazione verso l'applicazione dovrà sottostare agli stessi requisiti dell'accesso alla rete pubblica dei gestori di telecomunicazioni.

Classificazione dei dispositivi autorizzati ad accedere alle applicazioni mobile

La progettazione di un'applicazione mobile, al di là dell'indubbia comodità per l'utente di una *user experience* svincolata da una postazione fissa, pone dei problemi sulla regolamentazione del suo utilizzo onde rispettare i presupposti delle politiche di sicurezza dell'organizzazione: mentre un accesso logico da una postazione di lavoro è facilmente rintracciabile e localizzabile non si può dire altrettanto per gli accessi da terminale mobile.

Occorre prima di tutto verificare se la Struttura Sanitaria intende fornire l'accesso alle applicazioni mobile solo attraverso i dispositivi censiti di sua proprietà (situazione che consente un controllo molto approfondito se opportunamente configurato), solo attraverso i dispositivi mobili dei dipendenti e collaboratori (situazione che oltre a comportare problematiche importanti di privacy consente di esercitare un controllo minimo) oppure un mix delle due condizioni che andrà opportunamente disciplinata nella Mobile Security Policy.

In tutti i casi risulta di fondamentale importanza la registrazione degli *asset* e delle informazioni relative alle utenze associate cui è consentito l'accesso in mobilità ai servizi cui applicare, in funzione delle *policy* aziendali vigenti, le opportune misure di protezione.

Tecnologie di protezione dei dispositivi e delle applicazioni mobili (MDM e MAM)

Se i dispositivi mobili, *smartphone* e *tablet*, sono gestiti dall'azienda è possibile adottare delle soluzioni tecnologiche denominate Enterprise Mobile Management (EMM) in grado di attivare in modo uniforme e controllato delle politiche di protezione sui dispositivi che, a seconda del loro ambito di azione sono classificate come:

- **Mobile Device Management (MDM):** applicazione di gestione asset centralizzata che tiene aggiornato l'inventario dei dispositivi in termini di caratteristiche *hardware*, sistema operativo ed app installate, sovrintende agli aggiornamenti del *software* e dei prodotti *antimalware*, può consentire la localizzazione dei dispositivi ed, in caso di furto o smarrimento, permette di cancellare i dati *(remote wiping)* o di rendere il dispositivo inutilizzabile.
- **Mobile Application Management (MAM):** applicazione di gestione *asset* centralizzata che consente di gestire in modo selettivo le applicazioni installate sul dispositivo; nel caso di gestione di un *device* personale consente di abilitare una separazione netta tra l'utilizzo personale ed aziendale delle applicazioni attraverso l'uso di meccanismi di *sandboxing*. Nel caso di utilizzo "aziendale" si può richiedere un'autenticazione esplicita per utilizzare l'applicazione, si può restringere il *download* delle applicazioni solo dall'app store dedicato, effettuare alcuni controlli di sicurezza prima di avviarle, tracciarne l'utilizzo e cancellare remotamente i dati.

Sicurezza delle applicazioni mobili

Anche il settore delle applicazioni mobili non si sottrae alla dimostrata in-sicurezza delle applicazioni *software*: come emerge anche dai risultati del Top 10 Mobile Risks di OWASP sono ancora diverse le aree di miglioramento nell'ambito dello sviluppo di applicazioni *mobile*; in sintesi gli ambiti in cui risulta necessario un intervento urgente sono i seguenti:

- controlli da implementare lato server;
- validazione input lato client;
- gestione delle sessioni;
- protezione del codice eseguibile;
- problemi nella comunicazione cifrata (sia nella fase di trasporto, che nell'algoritmo di cifratura).

Di particolare rilievo per l'ambito sanitario, in virtù del livello di sensibilità dei dati potenzialmente trattati, risultano le problematiche relative all'autenticazione ed all'autorizzazione degli utenti oltre alla cifratura dei dati memorizzati, siano essi depositati su *file system*, su *data base*, oppure nelle aree di memorizzazione dei dispositivi mobile.

Verifiche di sicurezza

Risulta evidente come, a fronte della complessità sottostante la fruizione in mobilità delle applicazioni di tipo sanitario e della possibile appetibilità dei dati sensibili trattati, sia importante poter valutare a priori ed in modo quanto più oggettivo possibile il livello di sicurezza offerto dal sistema completo.

E' quindi opportuno effettuare, prima della messa in produzione e comunque in occasione di importanti cambiamenti, un test esaustivo *(Penetration Test)* del livello di sicurezza intrinseco dell'infrastruttura di accesso, dell'applicazione mobile e dei modelli di *smartphone* e *tablet* maggiormente utilizzati, in modo da simularne l'utilizzo in un ambiente dichiaratamente ostile.

Tale verifica andrebbe eseguita a cura di una terza parte in possesso di comprovate capacità tecniche con l'obiettivo di mettere in luce eventuali falle nel sistema di sicurezza e porvi rimedio prima che un attaccante possa farlo con impatti decisamente più importanti.

Monitoraggio del livello di sicurezza: perché attivarlo?

Nei sistemi informativi complessi ed eterogenei adottati dalle organizzazioni sanitarie è molto importante il monitoraggio del livello di sicurezza sia a fronte di possibili problemi che possano comportare la perdita della disponibilità dei servizi sia in caso di episodi che abbiano impatti su riservatezza ed integrità dei dati che, a fronte di episodi di *data breach*, possono comportare rilevanti sanzioni e richieste di risarcimento da parte degli individui coinvolti tali da minare la reputazione dell'azienda sanitaria.

Il punto di partenza per le attività di monitoraggio è l'analisi dei *file di log*: data la complessità dell'infrastruttura elaborativa questo può avvenire trasferendo i file di log e gli eventi di sicurezza su una piattaforma dedicata di *log management* che consente di velocizzare le operazioni oltre a consentire un'archiviazione a lungo termine delle suddette informazioni anche sotto il profilo forense.

Una evoluzione rispetto alle fasi di raccolta, normalizzazione, indicizzazione ed archiviazione dei file di log e degli eventi sopra citate è rappresentato dalla possibile integrazione di soluzioni SIEM (Security Information & Event Management) che consentono di correlare tra di loro gli eventi oltre che con altre informazioni quali dislocazione degli asset nelle sedi, amministratori di sistema coinvolti, il grado di criticità ecc.; questa caratteristica che consente di aggregare e contestualizzare meglio le informazioni, in modo da facilitare le attività di analisi.

La gestione degli incidenti di sicurezza informatica e le strategie di comunicazione da adottare

Onde fronteggiare in modo organico il verificarsi di un potenziale incidente di sicurezza informatica una organizzazione deve prima di tutto adottare una procedura di gestione, che fornisca precise indicazioni comportamentali agli attori coinvolti, in modo da affrontare la contingenza della situazione evitando reazioni dettate dal panico.

In quanto misura organizzativa il documento deve essere in *primis* condiviso dal *management* e deve contenere le indicazioni sulla composizione del Comitato operativo della struttura preposta alla Gestione della Crisi, formato dal responsabile della sicurezza informatica, dai referenti della gestione tecnica dei sistemi informativi, ma anche dai responsabili degli uffici privacy, legali, della comunicazione ed HR dell'organizzazione.

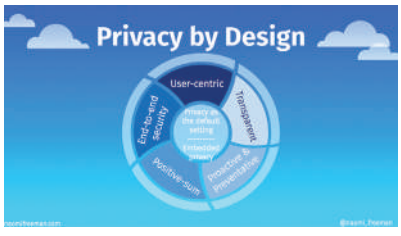
Il gruppo responsabile della gestione della crisi dovrà prevedere una lista di contatti di supporto esterno, tra cui la Polizia Postale, i provider dei servizi Internet, i Computer Emergency Response Team (CERT), eventuali strutture di supporto interne al mercato di riferimento e, nel caso in cui le competenze non fossero presenti, una società in grado di eseguire attività di computer forensics.

Le comunicazioni relative all'incidente informatico tra i membri del Comitato di Gestione Crisi dovranno avvenire attraverso dei canali prestabiliti sempre disponibili, mentre l'addetto alla comunicazione designato si occuperà delle relazioni verso i media, il personale interno e dell'eventuale utenza esterna.

Ai fini della valutazione della portata dell'incidente occorrerà definire a priori delle condizioni che comportino degli impatti significativi prima di innescare le procedure di gestione.

Conclusioni

E' stata fornita una panoramica delle problematiche che potrebbero avere un impatto negativo sui livelli di privacy e di sicurezza attesi da parte di un fruitore, sia interno che esterno, dei servizi offerti da un'azienda sanitaria tramite applicazioni mobile.



In accordo con il principio "security/privacy by design" che rappresentano uno dei punti chiave del Regolamento GDPR di prossima introduzione sono state suggerite alcune indicazioni che dovrebbero rappresentare misure di protezione adeguate; purtroppo, come si può evincere dalle statistiche pubblicate sugli episodi di *data breach*, siamo ancora molto lontani dal traguardo.

L'obiettivo dell'articolo è stato quello di dare una vista di insieme anche su elementi collaterali quali il monitoraggio della sicurezza e la gestione degli incidenti, fornendo degli spunti di riflessione su situazioni che spesso non vengono correttamente indirizzate nel corso di progetti che dovrebbero coniugare la possibilità di utilizzare le nuove tecnologie assicurando un opportuno livello di protezione onde salvaguardare la privacy del cittadino. ■

Sicurezza e Salute nell'era dell'Ospedale 4.0

Autori: Roberto Setola, Luca Vollero

Negli ultimi anni si è assistito a un crescente interesse verso l'impiego pervasivo di sistemi ICT in ambito medico con l'obiettivo di sviluppare servizi intelligenti che innalzino l'efficienza e la qualità dell'healthcare. Il concetto di Ospedale 4.0 (Hospital 4.0 - H4.0), declinazione del concetto di Industria 4.0 al mondo dell'ospedale, è l'istituzionalizzazione di tale trend. Nel modello Ospedale 4.0 questo fenomeno è sostanziato dall'introduzione di componenti IoT (Internet of Things – Internet delle cose) all'interno dei dispositivi e degli ambienti dell'ospedale, e dall'impiego di una crescente automazione a supporto dei servizi e dei processi di decisione e gestione dell'ospedale.

L'Ospedale 4.0 è un sistema dinamico in cui l'ambiente, i dispositivi e i processi dell'ospedale tradizionale vengono interfacciati con componenti interni ed esterni, a controllo diretto o indiretto dell'Ospedale. Tali componenti possono essere fisici (hardware) o computazionali (software) e il loro compito è generare/processare informazione e, nei casi più avanzati, realizzare scelte e avviare/controllare processi e macchinari. L'Ospedale 4.0 è, quindi, un sistema complesso, distribuito, dai confini sfumati e costituito da elementi fisici e cyber, ovvero è quello che in gergo tecnico viene detto ambiente cyber-fisico (CPS – Cyber-Physical System). All'interno di tale ambiente si muovono informazioni delicate legate non solo alla riservatezza e sicurezza (privacy e security) del paziente e del personale presente nell'Ospedale, ma anche all'incolumità (safety) degli stessi. La delicatezza delle informazioni gestite e la loro alta appetibilità da parte di terze parti criminali, rende il problema della sicurezza nell'Ospedale 4.0 di primaria importanza.

La natura cyber-fisica dell'Ospedale 4.0 rende tali sistemi particolarmente vulnerabili non solo sotto l'aspetto tecnico, ma anche sotto l'aspetto organizzativo e sociale. Infatti, l'estrema variabilità in termini di sistemi, protocolli e personale complica la creazione di un ambiente robusto contro gli eventi esterni e i comportamenti poco accorti degli utenti, e poco sicuro contro azioni deliberatamente criminali.

Le diverse minacce che l'Ospedale 4.0 deve poter fronteggiare possono essere di tre categorie principali: (i) minacce determinate da fenomeni esterni, (ii) minacce determinate da fattoti umani e (iii) minacce dovute a malfunzionamenti di alcuni sottosistemi.

Minacce determinate da fenomeni naturali o incidenti

Le minacce determinate da eventi esterni sono originate da fenomeni naturali (terremoti, alluvioni, incendi) o antropici (incidenti, guasti, ecc.) che, degradando il funzionamento di alcune componenti dell'Ospedale o delle infrastrutture esterne all'Ospedale, possono produrre degli effetti a cascata con

BIO

Luca Vollero si è laureato in Ingegneria delle Telecomunicazioni presso l'Università Federico II di Napoli nel 2001. Presso la stessa Università ha conseguito nel 2005 il Dottorato di Ricerca in Ingegneria Informatica e Automatica. Da luglio 2006 a ottobre 2014, ricopre il ruolo di ricercatore presso l'Università Campus Bio-Medico di Roma, mentre da ottobre 2014 è professore associato (settore ING-INF/05 Sistemi di Elaborazione delle Informazioni) presso la stessa università.

Luca Vollero ha partecipato e partecipa a diversi progetti di ricerca nazionali e regionali, coordinandone alcuni, su tematiche di telemedicina, affrontando problemi di usabilità, prestazioni e integrazione con sistemi ospedalieri tradizionali. Inoltre, collabora in qualità di docente al Master universitario di II livello in "Homeland Security: Sistemi, Metodi e Strumenti per la Security ed in Crisis Management". È autore di oltre 80 articoli su riviste e conferenze internazionali, ed è membro di molteplici comitati editoriali di riviste e di conferenze nazionali e internazionali.

BIO

Roberto Setola, PhD, è professore associato (settore ING-INF/04 Automatica) presso l'Università Campus Bio-Medico di Roma dove ricopre anche il ruolo di Direttore del Laboratori Sistemi Complessi e Sicurezza (www.coseritylab.it) ed è Delegato del Rettore per i rapporti con il mondo industriale.
È dal 2007 il Direttore Scientifico del Master universitario di II livello in "Homeland Security: Sistemi, Metodi e Strumenti per la Security ed in Crisis Management"; ed è stato dal 2014 al 2017 Presidente del Corso di Laurea in Ingegneria Industriale.
Dal 2018 è Direttore Generale del del Consorzio Nazionale Interuniversitario per la Logistica ed i Trasporti (NITEL).
Ha conseguito la laurea in Ingegneria Elettronica (1992) e poi il dottorato di ricerca in Ingegneria Elettronica Informatica (1996). Dal novembre 1999 al marzo 2004 è stato presso la Presidenza del Consiglio dei Ministri lavorando nell'ambito della progettazione e gestione di sistemi informativi complessi e dove, fra l'altro, è stato il responsabile della segreteria tecnica del Gruppo di Lavoro per la Protezione delle Infrastrutture Critiche Informatizzate e ha rappresentato il governo italiano in diversi consessi internazionali, fra cui G8, EU e NATO.
È stato il coordinatore scientifico di 4 progetti di ricerca internazionali co-finanziati dall'Unione Europea europei, dello studio per l'analisi dei rischi dei cantieri della linea ferroviaria Torino-Lione in Val di Susa ed è stato responsabile di una unità di ricerca in oltre 25 progetti di ricerca fra nazionali ed internazionali fra cui la Rete di Eccellenza CIPRNet per lo sviluppo di un centro europeo di analisi e simulazione di infrastrutture critiche.
È autore di 1 brevetto internazionale, 11 volumi (di cui 9 in lingua inglese) e di oltre 200 pubblicazioni scientifiche sui temi dell'automazione, della modellistica e controllo dei sistemi complessi e della sicurezza industriale.

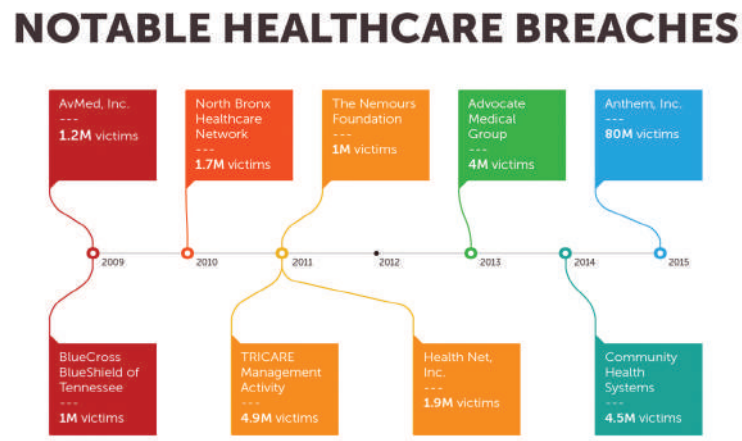
rapido deterioramento, se non cancellazione, dei servizi offerti. Tali scenari, che pur erano presenti anche in un Ospedale tradizionale, tendono ad essere amplificati in uno scenario di Ospedale 4.0 stante il maggior utilizzo di risorse esterne (soprattutto per quel che riguarda la comunicazione e l'accesso alle informazioni) ma anche alla luce della sempre più crescente presenza di servizi erogati sul territorio dall'Ospedale a partire dalle attività di tele-medicina.

Anche senza ipotizzare scenari catastrofici, occorre considerare come anche un semplice sovraccarico dei servizi di comunicazione, legato ad un guasto ovvero ad una anomalo aumento delle richieste, può avere su applicazioni di telemedicina, con la creazione di difficoltà che possono sfociare nell'impossibilità di garantire il costante monitoraggio dei parametri vitali, con conseguente necessità di "internalizzare" in via precauzionale i pazienti non più gestibili da remoto.

Ovviare a questo e altri problemi di questo tipo è una questione molto delicata in cui concorrono motivazioni e modelli di gestione diversi, un'approfondita analisi dei rischi che possono gravare sull'Ospedale e un'attenta valutazione dei costi.

Minacce determinate da fattori umani

Le minacce determinate da fattori umani includo minacce dirette e indirette determinate da persone che, volontariamente o involontariamente, creano condizioni di rischio per persone, dispositivi e servizi dell'Ospedale.



Le minacce dirette sono quelle che vengono determinate da persone o organizzazioni che deliberatamente, per i motivi più svariati, ma tipicamente a scopo di lucro, vogliono mettere a rischio gli asset dell'Ospedale. L'esempio più conosciuto di questa tipologia di rischio è costituito dai **Malware**, di cui i **ransomware** sono probabilmente la realizzazione più nota, più diffusa e, al momento, più rischiosa per il tipo di asset coinvolto. Gli attacchi **ransomware** sono un esempio emblematico di un vettore informatico il cui ingresso e diffusione all'interno dell'Ospedale è determinato da una congiunzione di vulnerabilità sociali, quali la cattiva preparazione dei dipendenti, e tecnologiche, quali sistemi di sicurezza non sufficienti e/o non sufficientemente aggiornati. I ransomware sono, però, solo una delle possibili tipologie di malware che possono diffondersi facilmente, sfruttando, ad esempio, la maggiore superficie di attacco informatica generata dalla diffusione del paradigma IoT, e arrecare danni all'Ospedale 4.0. Accanto ai ransomware, infatti, troviamo altri degni e altrettanto pericolosi compagni quali gli spyware, i worms, i trojan, i virus, i rootkit, gli exploitkit e le botnet.

Le minacce dirette non si limitano solo alla diffusione di software malevolo all'interno dei dispositivi dell'Ospedale, ma possono includere altre minacce anche molto gravi quali (i) la riprogrammazione non autorizzata dei dispositivi, specialmente quelli IoT, che può avvenire, ad esempio, durante le fasi di manutenzione all'esterno dell'ospedale, (ii) il furto di dispositivi e dati, (iii) attacchi di tipo DoS e DDoS, (iv) lo sniffing, (v) lo skimming e attacchi sociali.

Una considerazione particolare va fatto con riferimento alle minacce connesse con le Operational Technologies (OT) e più in generale con i dispositivi bio-medicali. Le OT sono quell'insieme di tecnologie hardware e software deputate alla supervisione e al corretto funzionamento di tutti gli impianti e delle principali apparecchiature di un Ospedale. I fenomeni di pervasiva diffusione dei sistemi ICT hanno fatto si che questi sistemi, un tempo operanti su reti e con protocolli e sistemi i solati proprietari, siano oggi fortemente interconnessi con la rete IT e quindi potenzialmente esposti alle minacce cyber. Per le loro peculiarità una eventuale compromissione cyber può comportare non solo una interruzione nell'erogazione dei servizi, con conseguente necessità di utilizzare sistemi ausiliari e/o di emergenza, ma anche un loro non corretto funzionamento che potrebbe avere un potenziale impatto sulla saluta dei pazienti e dei dipendenti. In questo contesto ancora più drammatica potrebbe essere la compromissione dei dispositivi biomedici con conseguente potenziale alterazione sia del risultato diagnostiche che di quello terapeutico.

Le minacce indirette occorrono per conseguenza di processi inadeguati e cattiva preparazione del personale e riguardano la cattiva configurazione o il cattivo utilizzo dei sistemi. Tale problema, già presente nell'ospedale tradizionale è esacerbato in un contesto di Ospedale 4.0, dove i cattivi comportamenti possono facilmente degenerare in disservizi o apertura di falle per attacchi di tipo diretto. L'esempio principe di una minaccia di questo tipo è l'impiego di dispositivi personali in zone protette, ovvero l'impiego del paradigma BYOD (Bring Your Own Device). Un dispositivo personale, per definizione, è un dispositivo esterno all'Ospedale che può, però, muoversi a stretto contatto con dispositivi interni e in zone in cui la sicurezza informatica è più blanda. Di conseguenza, un dispositivo personale compromesso è un vettore di infezione/vulnerabilità particolarmente delicato e difficilmente controllabile.

Ovviare alle minacce determinate da fattori umani è particolarmente complicato per l'estrema variabilità che questo tipo di minacce può presentare. Da una parte è necessario prevedere fasi di preparazione e aggiornamento periodico del personale dell'Ospedale. Dall'altra, è auspicabile un continuo aggiornamento e verifica dei sistemi e dei processi dell'Ospedale e un controllo stringente su tutti quei vettori che, inconsapevolmente, possono essere condotti in aree delicate dell'ambiente ospedaliero. Questa attività deve includere anche i fornitori dell'Ospedale al fine di evitare che eventuali comportamenti non adeguati commessi al di fuori del perimetro fisico dell'Ospedale possa introdurre all'interno dello stesso significative problematiche di sicurezza.

Minacce determinate da malfunzionamenti

L'Ospedale 4.0 è un sistema di componenti variamente interconnessi e interdipendenti. Data l'alta interconnessione, malfunzionamenti di componenti isolati possono facilmente degradare in disservizi di grande entità, con compromissione di servizi anche delicati. In tale contesto bisogna distinguere due grandi categorie di malfunzionamenti: i malfunzionamenti determinati da sistemi interni e malfunzionamenti determinati da sistemi esterni. I primi riguardano componenti sotto il controllo diretto dell'Ospedale e includono (i) la caduta di servizi software (PACS, software amministrativo, …), (ii) la caduta di sistemi hardware e (iii) di interconnessione interna e (iv) il sovraccarico dei sistemi.

Spesso tali malfunzionamenti sono collegati a cattive politiche di monitoraggio, manutenzione e aggiornamento.

La seconda tipologia di malfunzionamenti è determinata da sistemi esterni che offrono servizi all'Ospedale quali la fornitora di elettricità, di servizi Internet e di servizi cloud. Ovviamente una sospensione temporanea, parziale o completa, fortuita o dolosa, di questi servizi ha delle ricadute su un Ospedale in cui la componente digitale diventa sempre di più il motore del suo funzionamento. Ovviare alla prima tipologia di minacce richiede forti investimenti da parte del sistema Ospedale per dotarsi e alimentare una struttura di monitoraggio, controllo, gestione e reazione alle minacce riguardanti tutti i sistemi sotto il suo controllo. Per mitigare l'impatto di disservizi esterni, l'Ospedale deve dotarsi di una certa autonomia sistemica (gruppi di continuità, duplicazione interna di porzioni di servizi esterni, …) con costi di apparati e di gestione che devono essere oggetto di un'attenta analisi costi/benefici.

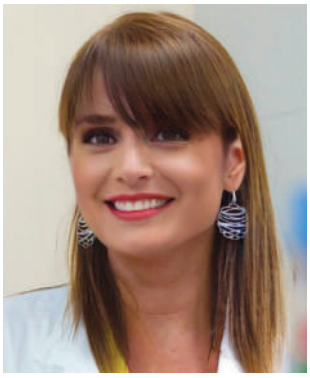
Considerazioni

Il paradigma dell'Ospedale 4.0 rappresenta una grande opportunità per migliorare e contemporaneamente rendere più efficienti i servizi del mondo healthcare. La profonda trasformazione che questo paradigma comporta nel modello di Ospedale tradizionale, però, incrementa il livello di fragilità che questa tipologia di sistemi presenta. Una superficie di attacco più ampia, una forte interdipendenza dei sistemi, la presenza del fattore umano sono gli elementi principali che concorrono a questa fragilità. Il tema della sicurezza è sicuramente quello più delicato e sul quale, dopo una prima fase di sottovalutazione, ci si sta rendendo conto di dover investire maggiormente anche se lo scenario nazionale e internazionale desta ancora forte preoccupazione. ■

eHealth: molti successi ma attenti a non perdere di vista il paziente, il quale diventa un numero e non più una persona

Intervista VIP a Antonella Viola

Autore: Massimiliano Cannata



Antonella Viola

Quali sono i progetti attuali dell'istituto che dirige e che vedono un uso centrale della tecnologia?

Tutti i progetti attivi all'interno dell'Istituto di Ricerca Pediatrica Città della Speranza sono fortemente incentrati sulla tecnologia e l'innovazione. L'utilizzo di strumenti all'avanguardia è indispensabile per le analisi dei campioni biologici, così come software sofisticati sono fondamentali per l'analisi e l'interpretazione dei dati. La tecnologia è applicata quindi alla diagnostica avanzata, sia in campo oncologico sia genetico, ma anche ai progetti di ricerca di bioingegneria per la rigenerazione di tessuti o a quelli per le terapie innovative basate su nanoparticelle. Un esempio concreto? Il gruppo di medicina rigenerativa sta lavorando allo sviluppo di un bioreattore che permetta la creazione di un diaframma, in modo da offrire una terapia nuova ai bambini che nascono con malformazioni di questo tessuto. Per farlo lavorano fianco a fianco biotecnologi e ingegneri e utilizzano approcci molto sofisticati.

Quali sono le attese nel mondo medico relativamente ai vantaggi della tecnologia in campo diagnostico e clinico?

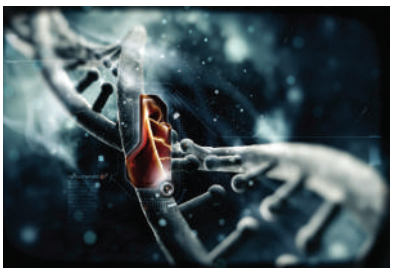
Sono altissime, in quanto è grazie alla tecnologia che si potrà permettere l'identificazione sempre più precoce dei marcatori di una malattia, senza i quali i pazienti non potrebbero usufruire di trattamenti mirati e sempre più efficaci. Ciò vale non solo relativamente ai test di laboratorio, ma anche per quanto riguarda esami clinici come TAC e PET. Oggigiorno, inoltre, lo sviluppo tecnologico consente di condividere piattaforme on-line per la revisione centralizzata dei casi e per un più accurato inquadramento diagnostico.

IBM ha sviluppato un sistema, chiamato Watson, in cui un'intelligenza artificiale effettua diagnosi su pazienti più accurate di quelle dei medici in carne ossa. E secondo l'autore di Homo Deus, gli algoritmi sempre più intelligenti sostituiranno l'essere umano in un tempo non lunghissimo anche in professioni altamente specializzate quali quella medica: lo ritiene possibile?

Non saprei, la tecnologia avanza così velocemente che è molto rischioso azzardare previsioni, in un senso o nell'altro. Certamente l'ausilio di strumenti efficienti e di precisione, a disposizione anche dei medici di base, cambierà la medicina e il metodo di lavoro del medico. Un algoritmo ha conoscenza e memoria altamente potenziate e in alcuni casi specifici può essere di grande aiuto nell'effettuare una diagnosi o nell'individuazione di una strategia terapeutica. Ma credo che siamo ancora lontani dallo scenario descritto dal libro.

Qual è stato a oggi il più grande successo conseguito dalla tecnologia in campo medico a suo avviso?

Sono molti. Tra questi: l'utilizzo della stampa tridimensionale capace di ricostruire i tessuti biologici con cellule; lo sviluppo delle scienze «omiche», le nanotecnologie. Le scienze «omiche» utilizzano tecnologie di analisi che consentono la produzione di grandi quantità di dati utili per la descrizione e l'interpretazione del sistema biologico studiato. Comprendono: la genomica, che analizza il DNA; la trascrittomica che invece analizza RNA; l'epigenomica che analizza come il DNA viene utilizzato; e la proteomica, che fornisce informazioni sulle proteine. Ma si arriva anche alla «Colturomica» in cui si analizzano per



esempio i vari tipi di batteri o del microbiota intestinale. Tutte queste tecnologie sono estremamente potenti per la quantità di dati che generano ma ovviamente richiedono di grandi competenze di analisi bioinformatica per poter trasformare i dati in informazioni. In ambito chirurgico, l'avvento di telecamere, sonde e interventi robotizzati ha sicuramente permesso di effettuare operazioni in maniera molto meno invasiva e precisa, e quindi garantire tempi di recupero più brevi e meno dolorosi per i pazienti. In ambito pediatrico, ne ha enormemente beneficiato l'oncologia perché ha permesso di identificare le mutazioni presenti nei singoli pazienti e di poter quindi facilitare il percorso terapeutico individuale. Il cancro non è tutto uguale e conoscere il nemico rende possibile mettere da subito in campo le armi giuste per combatterlo. La diagnostica avanzata si basa appunto su questo: identificare le mutazioni del paziente, associarle sulla base delle conoscenze scientifiche ad un rischio maggiore o minore, e procedere quindi attraverso approcci terapeutici specifici. La medicina personalizzata di cui tanto si parla consiste essenzialmente in questo.

Quali sono i rischi maggiori connessi all'uso della tecnologia in medicina?

Come in tutti gli ambiti, la tecnologia va gestita e utilizzata in maniera coerente. Teniamo presente che molte volte i pazienti hanno anche bisogno di essere ascoltati, che un bravo medico deve saper leggere tra le righe, che una serie di manifestazioni e sintomatologie sono spesso ascrivibili a stati di ansia, depressione. Forse tra i rischi maggiori vi può essere quello di perdere di vista il paziente, il quale diventa un numero e non più una persona.

Vediamo spesso usare la tecnologia per abbreviare la comunicazione, come nel resto del mondo sociale: spesso il medico si fa mandare il referto via mail o la foto dello sfogo cutaneo via whatsapp per capire se è il caso di visitare o se non c'è nulla di cui preoccuparsi. Questo accorciarsi delle distanze, che appunto rispecchia quanto accaduto anche nel resto del mondo, è un bene o un male in una scienza quale la medicina, che a volte richiede forse più sfumature di quelle delle emoji di Whatsapp o di una ricerca nell'archivio di Medicitalia?

Di nuovo, il problema non è la tecnologia ma il suo utilizzo. La velocità della comunicazione è essenziale per mettere in rete i vari centri di ricerca, i vari ospedali, per fornire diagnosi in tempo reale. Noi per esempio siamo un centro di riferimento nazionale per i tumori infantili: questo significa che ogni giorno riceviamo dei prelievi dagli ospedali di tutta l'Italia e grazie alla tecnologia possiamo inviare il risultato delle nostre analisi al medico curante senza che il paziente si sposti. Ma naturalmente questa facilità di comunicazione deve essere gestita nel modo corretto. Il paziente non può essere curato on-line. ■

BIO

Antonella Viola è Professoressa Ordinaria di Patologia Generale presso il Dipartimento di Scienze Biomediche dell'Università di Padova e Direttrice Scientifica dell'Istituto di Ricerca Pediatrica (IRP-Città della Speranza www.cittadellasperanza.org). Ha coordinato diversi progetti di ricerca nazionali, europei e americani finalizzati allo studio del sistema immunitario e del cancro. E' stato membro del comitato scientifico dell'Associazione Italiana Ricerca sul Cancro (AIRC) ed è revisore per la Commissione Europea dei progetti europei di eccellenza scientifica (ERC). Per il suo contributo all'immunologia ha ricevuto numerosi riconoscimenti tra cui il premio Roche, il premio del Cancer Research Institute of New York, il premio Chiara D'Onofrio, il premio Young Investigator dell'European Molecular Biology Laboratories (EMBO), il grant dell'European Research Council come Advanced Investigator. Nel 2016, per il suo eccezionale contributo alla biologia molecolare, è stata nominata membro della "European Molecular Biology Organization" (EMBO), prima donna dell'Università di Padova e di tutto il Nord-Est. La prof.ssa Viola è stata invitata a tenere conferenze in centri di ricerca di tutto il mondo, tra cui Imperial College di Londra, Institut Pasteur a Parigi, Harvard Medical School a Boston, Università di Oxford, Medical Research Council di Cambridge, Jefferson University di Philadelphia e molti altri. Attualmente, coordina un progetto europeo su infiammazione (ERC AdG STePS) ed è workpackage leader di un progetto europeo sul trapianto di staminali nelle malattie infiammatorie croniche del fegato (FP7 MERLIN).
In aggiunta alla sua attività didattica e di ricerca, Antonella Viola si occupa attivamente di divulgazione scientifica. Ha fatto parte del progetto europeo #EuFactor http://www.eufactor.eu/ (https://www.youtube.com/watch?v=EdamCzKcvHQ), speaker TEDx Padova (https://www.youtube.com/watch?v=bXGFEdxzzco) (https://www.youtube.com/watch?v=WCCuSntj8AY), ospite di diverse testate televisive e di manifestazioni culturali e divulgative in tutto il paese. Dal 2017 è un socio onorario del CICAP (Comitato Italiano per il Controllo delle Affermazioni sulle Pseudoscienze). Tra i premi dedicate a donne eccellenti ha ricevuto il premio "Nilde Iotti" e il premio "Donne Eccellenti" della fondazione Belisario; fa inoltre parte delle "100 donne contro gli stereotipi" della Fondazione Bracco https://100esperte.it/. Ha ideato e organizzato il progetto di divulgazione scientifica "Viaggio al Centro della Scienza".

eHEALTH: istruzioni per l'uso

Autore: Giancarlo Butti

I vantaggi dei servizi legati all' eHEALTH sono concreti ed innumerevoli, ma troppo spesso ci si dimentica di un rilevante fattore di rischio: l'utente.

Il Ministero della salute cita fra i servizi offerti in ambito eHEALTH il *CUP - Centro Unico di Prenotazione*, il FSE - *Fascicolo Sanitario Elettronico*, i *Certificati telematici di malattia*, la *ePrescription - Ricetta medica elettronica*, la *Telemedicina*.

Oltre a questi, sotto il cappello di *eHEALTH* è possibile citarne altri, facilmente reperibili in letteratura, quali l'*interoperabilità tra sistemi*, il *consumer health informatics*, il *virtual healthcare teams* e molti altri ancora, in funzione della fonte e delle modalità di classificazione…

Recentemente ho avuto modo di sperimentare per alcuni mesi, come paziente, più o meno tutti i servizi di *eHEALTH* offerti dal nostro Servizio Sanitario e ho trovato alcuni aspetti positivi ed altri decisamente migliorabili.

È infatti un po' anomalo che il servizio di prenotazioni per via telematica o per operatore funzioni perfettamente se hai necessità dilazionabili nel tempo, ma non sia in grado di gestire le emergenze, e cioè una richiesta di visita in tempi molto rapidi per la cui prenotazione è richiesta la presenza fisica (questa almeno è stata la mia esperienza).

Anomalo anche il fatto che ho dovuto rifare la fila più volte per prenotare o pagare (se già prenotato per via telematica) due diversi tipi di intervento nello stesso giorno in quanto lo sportello non era abilitato ad eseguire entrambe le prenotazioni.

Ancora più anomalo il fatto che per poter accedere a due sportelli diversi ho dovuto utilizzare due causali diverse, pur dovendo fare la stessa cosa, in quanto il sistema impedisce, ad esempio, di effettuare la gestione di più di una lista di attesa al giorno (situazione che può invece presentarsi se un paziente dopo aver pagato una prestazione già prenotata – ad esempio una visita di controllo - ed averla effettuata di lì a poco, deve procedere a prenotare/pagare una nuova visita che gli è stata prescritta al momento).

Trovo invece decisamente molto comodo ricevere sul proprio fascicolo sanitario i risultati delle analisi in formato elettronico, anche perché, in quanto donatore di sangue, questo avviene con una certa frequenza.

Debbo dire tuttavia che sono abbastanza terrorizzato all'idea che tutte le informazioni relative alla mia salute siano presenti in un unico punto, accessibile telematicamente da diversi soggetti.

Il fatto di poter teoricamente gestire i livelli di accesso di tali soggetti non mi tranquillizza più di tanto (informazione questa che mi è nota solo in quanto ho affrontato il tema del FSE dal punto di vista del rispetto della normativa privacy, ma che ritengo sia ignota ai più) e la possibilità che un incidente di sicurezza possa rendere pubbliche le informazioni sullo stato di salute di migliaia di cittadini è decisamente inquietante.

Tralasciamo in questo articolo aspetti di sicurezza quali la disponibilità o l'integrità del dato, che ancor più della confidenzialità, possono avere esiti nefasti sul soggetto interessato in caso di incidente di sicurezza.

BIO

Giancarlo Butti (LA BS7799, LA ISO/IEC27001, CRISC, ISM, DPO, CBCI, AMCBI) ha acquisito un master di II livello in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80 ricoprendo diversi ruoli: security manager, project manager ed auditor presso gruppi bancari; consulente in ambito sicurezza e privacy presso aziende dei più diversi settori e dimensioni. Affianca all'attività professionale quella di divulgatore, tramite articoli, libri, white paper, manuali tecnici, corsi, seminari, convegni. Svolge regolarmente corsi in ambito privacy, audit ICT e conformità presso ABI Formazione, CETIF, ITER, INFORMA BANCA, CONVENIA, CLUSIT, IKN… Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate tradizionali ed una decina on line. Ha pubblicato 21 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 7 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT... È socio e proboviro di AIEA, socio del CLUSIT e del BCI. Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity e Rischio Informatico, di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su frodi, GDPR, eidas, sicurezza dei pagamenti…, di UNINFO sui profili professionali privacy, di ASSOGESTIONI sul GDPR. È membro della faculty di ABI Formazione, del Comitato degli esperti per l'innovazione di OMAT360 e fra i coordinatori di www.europrivacy.info .

La eHEALTH ha quindi molti vantaggi, ma sicuramente introduce quella serie di rischi tipici di una gestione informatizzata del dato, che nel caso in specie, considerando i possibili impatti di una loro violazione, meritano una costante attenzione e misure di sicurezza rilevanti che tuttavia, come chiunque si occupi di tale argomento ha ben presente, non sono infallibili.

Francamente mi sarei sentito più sicuro se i vantaggi della concentrazione di informazioni sulla mia salute, invece che essere centralizzati, fossero presenti su un dispositivo in mio possesso, opportunamente cifrato ed accessibile solo con una combinazione di chiavi anche sotto il mio controllo (ad esempio un mio dato biometrico).

A dire il vero la disponibilità di dati sanitari in formato elettronico o la loro disponibilità on line non è un fatto nuovo, ma una realtà con cui siamo abituati a confrontarci da parecchi anni; tuttavia troppo spesso ci si dimentica di considerare quello che è il punto debole della catena: il livello di consapevolezza dell'utente/paziente.

Di fatto il livello di attenzione dell'utente medio nel trattare i propri dati sanitari in formato digitale è di molto inferiore a quello, già scarso, con cui lo stesso tratta i dati relativi ai propri rapporti finanziari.

Mentre tuttavia almeno sul lato finanziario le singole banche e le associazioni di settore hanno promosso diverse campagne di sensibilizzazione, sul mondo specifico dei dati sanitari nulla è stato fatto.

Non sempre inoltre le controparti dell'utente sono all'altezza della situazione. Queste possono essere rappresentate da strutture sanitarie più o meno articolate e complesse, da singoli medici ed operatori sanitari ed anche dalle assicurazioni, alle quali richiedere rimborsi per un infortunio o malattia.

La modalità di interazione con tali soggetti non sempre prevede l'uso di canali di comunicazione cifrati e di credenziali personali.

Recentemente ho dovuto inoltrare lo stesso documento sanitario a due diverse compagnie assicurative; in un caso tramite una specifica piattaforma, nell'altro mediante l'uso di una semplice mail.

Il problema nel caso in specie non è soltanto legato al canale di comunicazione, e cioè al fatto che i miei documenti sanitari hanno viaggiato in chiaro tramite uno strumento tutt'altro che affidabile quale la posta elettronica.

È l'intero processo che presenta delle criticità che l'utente medio non percepisce, ma che mettono a repentaglio la confidenzialità dei suoi dati. L'uso della posta elettronica in luogo di una piattaforma dedicata fa sì che lato utente il documento sanitario sia presente sul pc del mittente non solo in qualche cartella, ma anche nel repository della posta elettronica (e forse su qualche server intermedio, come quello dei provider di appoggio…).

Analogamente avverrà presso il soggetto destinatario della compagnia assicurativa che, presumibilmente, dovrà estrarre tale documento dalla posta elettronica ed archiviarlo nel proprio sistema di gestione delle pratiche attive (si spera, cifrato). Quindi il documento sanitario è presente in un numero di copie eccessivo rispetto alla reale necessità (in violazione fra gli altri del principio di minimizzazione previsto sia dal vecchio Codice privacy, sia dal GDPR), in file allocati su sistemi ed applicativi diversi.

Lato utente potrei anche avere l'accortezza di proteggere il documento conservandolo in una cartella crittografata e potrei fare altrettanto con il file della posta elettronica, ma non ho alcuna confidenza su come lo stesso viene gestito dalla compagnia.

Inoltre un tale livello di sofisticazione nella conservazione dei file è piuttosto raro. La maggior parte degli utenti non si pone il problema di proteggere un file; pochissimi si pongono il problema di crittografare il file della posta elettronica, una volta che questa sia stata scaricata in locale…

Si corre quindi concretamente il rischio che un utente medio conservi sul proprio pc, senza alcuna protezione, i documenti sanitari che ha scaricato ad esempio dal proprio fascicolo sanitario, o che ha digitalizzato per l'inoltro ad esempio alla propria compagnia assicurativa.

Quest'ultimo aspetto merita un ulteriore punto di attenzione.

Anche se abbastanza diffuse, multifunzioni o scanner domestici non sono una dotazione standard di tutti gli utenti. Spesso l'acquisizione dell'immagine di un documento avviene mediante il proprio smartphone, oppure mediante le attrezzature disponibili in ufficio.

Al riguardo di queste ultime, pochi valutano il fatto che tali dispositivi dispongono di un disco su cui tali informazioni restano registrate, di solito fino a sovrascrittura, e che quindi sono virtualmente disponibili ed accessibili ad altri soggetti, quali ad esempio chi effettua la manutenzione e, virtualmente, al proprio datore di lavoro.

È evidente che anche in precedenza un utente/paziente conservava le proprie cartelle sanitarie.

Queste tuttavia, essendo su carta o altri supporti analogici quali le radiografie, non erano un possibile oggetto di violazione (salvo il rarissimo caso di un furto).

La disponibilità di tali informazioni, che crescerà in misura esponenziale in futuro, su dispositivi solitamente poco sicuri e facilmente accessibili aumenta notevolmente il livello di rischio.

Il livello di consapevolezza cala ulteriormente allorché si faccia uso di dispositivi autogestiti per la rilevazione di qualche parametro, quali ad esempio la pressione, che si interfacciano con il proprio smartphone e/o con sistemi centralizzati che permettono di storicizzare l'andamento nel tempo del parametro in questione.

Ma perché è così importante proteggere tali informazioni e creare consapevolezza negli utenti/pazienti?

Un dato sanitario può creare discriminazione: il rifiuto del rinnovo di un'assicurazione, la limitazione del proprio percorso di carriera, la diffidenza di colleghi e vicini di casa…

Non è quindi sufficiente che chi tratta dati sanitari, in particolare le istituzioni, adottino tutte le misure di sicurezza utili alla loro protezione, è necessaria una importante opera di sensibilizzazione e formazione degli utenti/pazienti su come gli stessi debbano gestire tali informazioni una volta che queste siano uscite dall'ambiente protetto[1] delle strutture sanitarie. ■

1 Non è oggetto di questo articolo indagare su questo aspetto; un dato eccezionalmente inquietante è tuttavia la irrisoria retribuzione prevista per un DPO presso un ASST

La Direttiva NIS: un articolato quadro tecnico-normativo

Autore: Gianluca Bocci

Tra il 2017 e il 2018 gli Stati Membri dell'Unione Europea, a fronte dei regolamenti e delle direttive emanate nel 2016 dal legislatore europeo, hanno operato importanti interventi normativi di adeguamento che hanno interessato istituzioni nazionali ma anche imprese pubbliche e private.

In tale ambito, i sistemi di pagamento elettronici con la direttiva PSD2, la nuova formulazione di un testo sulla tutela della privacy con il regolamento GDPR, e non per ultimo la sicurezza delle reti e dei sistemi informativi nell'Unione con la direttiva NIS, sono state alcune delle più importanti novità recepite nei sistemi giuridici nazionali.

BIO

Gianluca Bocci, laureato in Ingegneria Elettrica presso l'Università La Sapienza di Roma ha conseguito un Master Universitario di 2° livello presso l'università Campus Bio-Medico di Roma in "Homeland Security - Sistemi, metodi e strumenti per la Security e il Crisis Management". Attualmente è Security Professional Master nella funzione Tutela delle Informazioni di Tutela Aziendale, nella direzione Corporate Affairs di Poste Italiane. Certificato CISM, CISA, Lead Auditor ISO/IEC 27001:2013, Lead Auditor ISO/IEC 22301:2012, CSA STAR Auditor e ITIL Foundation v3, supporta le attività del CERT e del Distretto Cyber Security di Poste Italiane; in tale ambito ha maturato una pluriennale esperienza nella sicurezza delle applicazioni mobili, anche attraverso attività di ricerca e sviluppo realizzate con il mondo accademico. Precedentemente, presso importanti multinazionali ICT, in qualità di Security Solution Architect, ha supportato le strutture commerciali nell'ingegneria dell'offerta tecnico-economica per Clienti di fascia enterprise, con particolare riferimento ad aspetti di Security Information and Event Management, Security Governance, Compliance e Risk Management.

L'obiettivo di quest'articolo è di fornire quegli elementi utili per inquadrare i punti essenziali e per alcuni versi lo stato dell'arte della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 Luglio 2016 (a cui ci si riferirà d'ora in avanti con il termine "Direttiva") recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione Europea, anche nota come direttiva NIS (Network and Information Security); si terrà altresì conto di come la Direttiva è stata finora recepita e attuata in Italia con il Decreto Legislativo 18 Maggio 2018 n°65 (a cui ci si riferirà d'ora in avanti con il termine "Decreto"), pubblicato sulla G.U. del 9 Giugno 2018, n. 132.

La Direttiva, entrata in vigore a Maggio del 2016, è il risultato della definitiva comprensione da parte del Parlamento Europeo e del Consiglio, dell'importanza del ruolo che le reti e i sistemi informativi hanno per il benessere sociale ed economico dell'Unione, soprattutto in una dimensione transnazionale e di forte interdipendenza che caratterizza gli Stati membri, data la continua evoluzione e imprevedibilità della minaccia cybernetica che esaspera sempre di più lo scontro asimmetrico che vede contrapposti attaccante e difensore, rendendo necessario un intervento continuo e concreto del legislatore sovranazionale e nazionale.

E' di Repubblica[1] un articolo dal quale emerge che oltre mezzo miliardo di account sono stati rubati nel mondo e poco meno di 18 milioni di domini sono stati violati; poco più di 11 milioni sono state le credenziali di accesso (username e password) sottratte ad organizzazioni italiane e poco meno di 300 mila i domini compromessi a seguito di un attacco informatico nell'ultimo anno. In tal senso circa l'1,6% dei totali *"data breach"* ha interessato i domini italiani come il 2% delle credenziali complessive sono riconducibili ad account italiani. Dallo stesso articolo, dagli studi cui si riferisce ma in generale dai tanti report disponibili in rete, emergono molti altri dati interessanti che meritano di essere approfonditi per comprendere la reale entità della minaccia cibernetica; è proprio in questo scenario che la Direttiva pone obblighi in capo agli Stati membri affinché si dotino di un livello comune elevato di sicurezza delle reti e dei sistemi informativi per migliorare la propria capacità di difesa cibernetica, gestire in maniera adeguata i rischi e gli incidenti informatici e sviluppare programmi di cooperazione strategica per essere costantemente aggiornati sulle nuove minacce, vulnerabilità e tecniche di attacco. In tal senso, fermo restando il principio di autonomia garantito dalla Direttiva stessa, sia per le parti istituzionali coinvolte di ogni

Stato membro, sia le imprese interessate dal provvedimento, ci sarà un vero e proprio obbligo di adeguamento per perseguire gli obiettivi sopra menzionati, senza che essi vengano a collidere con quelle che sono le esigenze di Sicurezza nazionale.

Per una corretta interpretazione della NIS, occorre ricordare che la Direttiva non rappresenta "la strategia" dell'Unione Europea per la sicurezza cibernetica, piuttosto ne rappresenta un "elemento" importante con il quale per la prima volta è stato imposto agli Stati Membri di adottare un modello di governance.

Tale modello codifica e articola da un punto di vista organizzativo, strategico e operativo, la realizzazione di livello comune di sicurezza della rete e dei sistemi informativi nell'Unione e, in ultima analisi, ha l'obiettivo di migliorare il funzionamento del mercato interno (digital trust). Fatta questa premessa di seguito sono elencati gli aspetti salienti della Direttiva e, per quanto possibile, come la stessa è stata recepita in Italia. La Direttiva coinvolge un discreto numero di soggetti, alcuni anche con funzioni e caratteristiche indipendenti rispetto agli Stati membri altri che invece prevedono l'esplicito coinvolgimento di autorità pubbliche e imprese private.

Gruppo di cooperazione – Commissione Europea, ENISA e Stati Membri

Tra i principali soggetti istituiti dalla Direttiva per ottenere un avanzato e comune livello di sicurezza delle reti e dei sistemi informativi troviamo il c.d. *"gruppo di cooperazione[2]"* che, a livello europeo, è composto dalla *Commissione Europea, dall'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e dai rappresentanti degli Stati membri,* con l'obiettivo di sostenere e agevolare la cooperazione strategica e lo scambio d'informazioni tra gli Stati stessi. Al riguardo l'Italia con l'art.1, comma 2, lettera "d" del Decreto, stabilisce che il proprio ruolo nel gruppo di cooperazione è garantito dal Dipartimento delle informazioni per la sicurezza della Repubblica (DIS) in qualità di ***punto di contatto unico***, così come indicato nell'art.7, comma 3 e 5 dello stesso Decreto. Al gruppo di cooperazione sono presenti la Francia con l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), la Germania con l'Ufficio Federale per la Sicurezza delle Informazioni (Bundesamt für Sicherheit in der Informationstechnik), la Spagna con il Consiglio di Sicurezza Nazionale – Dipartimento di Sicurezza Nazionale (Consejo de Seguridad Nacional – Departamento de Seguridad Nacional) e così via molti altri paesi; tuttavia è bene sottolineare che non ancora tutti gli Stati membri al momento hanno istituito il proprio Punto di contatto unico.

Rientrano tra i principali obiettivi del gruppo di coordinamento, la condivisione di best practices e lo scambio d'informazioni sulle modalità di notifica degli incidenti, il supporto alla creazione di "capabilities" in materia di sicurezza anche attraverso l'attuazione di programmi di ricerca e sviluppo, gli schemi di sensibilizzazione e di formazione, sui fattori di rischio e in generale la capacità e lo stato di preparazione di ciascun Stato membro, i modelli che caratterizzano le strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi oltre all›efficacia dei CSIRT. Da quando è stato istituito, il gruppo di cooperazione ha pubblicato documenti d'interesse, quali:

- il *Reference document on security measures for Operators of Essential Services[3] (pubblicato a Gennaio 2018)*;
- il *Reference document on incident notification for Operators of Essential Services, circumstances of notification[4] (pubblicato a Febbraio 2018) con il quale, in linea con l'art. 14, comma 3 e 4 della Direttiva, s'intende*;
- il *Compendium on cyber security of election technology[5] (pubblicato a Marzo 2018);*
- il *Cybersecurity incident taxonomy[6] (pubblicato ad Aprile 2018);*
- la *Guidelines on notification of Operators of Essential Services incidents, formats and procedures[7] (pubblicato ad Maggio 2018);*
- la *Guidelines on notification of Digital Service Providers incidents, formats and procedures[8] (pubblicato ad Giugno 2018);*
- il *Reference document on the identification of Operators of Essential Services, modalities of the consultation process in cases with cross-border impact[9] (pubblicato ad Luglio 2018).*

A beneficio degli Stati membri questi documenti intendono promuovere un approccio convergente nell'adozione di principi e misure di sicurezza durante la fase di adozione e trasposizione a livello nazionale delle disposizioni previste dalla Direttiva, a prescindere dai gradi di libertà previsti con l'art.14, comma 1 e 2 della Direttiva, recepiti in maniera paritetica con l'art. 12, comma 1 e 2 del Decreto.

Operatori di servizi essenziali, fornitori di servizi digitali e Autorità Competenti

Nei documenti citati si fa riferimento ai c.d. *operatori di servizi essenziali e fornitori di servizi digitali;* i primi sono tutti quei soggetti che forniscono un servizio essenziale per il mantenimento delle attività economiche e/o sociali, la cui fornitura dipende proprio dalla rete e dai sistemi informativi e in tal senso potrebbe essere compromessa da un incidente, i secondi sono invece quelli che forniscono servizi di **e-commerce, cloud computing e motori di ricerca**.

Gli operatori di servizi essenziali e i fornitori di servizi digitali non sono individuati direttamente dalla Direttiva; i criteri e l'onere per identificarli rimangono in capo a ciascuno Stato membro. Le categorie che rientrano nell'ambito di applicazione della Direttiva sono per quanto concerne gli operatori di servizi essenziali quelli dell'energia, dei trasporti, delle banche, dei mercati finanziari, della sanità, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali; in Italia con l'art. 4, comma 1 del Decreto, le categorie e sottocategorie dovevano essere individuate entro il 9 Novembre 2018 dalle autorità competenti NIS che, previste nell'art.8 della Direttiva, sono state identificate, così come indicato nell'art.7, comma 1 del Decreto, nei seguenti dicasteri:

- il *Ministero dello Sviluppo Economico*, per il settore energia (energia elettrica, gas e petrolio), le infrastrutture digitali (IXP, DNS e TLD) e per i fornitori di servizi digitali (mercato on line, motori di ricerca online e servizi di cloud computing);
- il *Ministero delle Infrastrutture e dei Trasporti*, per il settore trasporti (aereo, ferroviario, per vie d'acqua e su strada);
- il *Ministero dell'Economia e Finanze* in collaborazione con *Banca d'Italia e Consob*, per il settore bancario e le infrastrutture dei mercati finanziari;
- il *Ministero della Salute* per il settore sanitario (istituti sanitari compresi ospedali e cliniche private);
- il *Ministero dell'Ambiente e della Tutela del territorio e del Mare*, le *Regioni* e le *Provincie Autonome di Trento e Bolzano* per il settore della fornitura e distribuzione di acqua potabile.

In ultima analisi in Italia, per quanto riguarda le Autorità Competenti in materia Cyber con i relativi aspetti di vigilanza e sanzionatori, si è deciso di adottare un modello decentralizzato in analogia a quello di alcuni paesi nordici come ad esempio la Svezia. Stante il ritardo nell'identificazione degli operatori di servizi essenziali e dei fornitori di servizi digitali, grazie alla Direttiva tali soggetti dovranno necessariamente adottare misure tecniche e organizzative adeguate per comprendere e gestire i rischi attraverso processi e tecnologie in grado di garantire la resilienza delle reti e dei sistemi informatici e dunque la continuità operativa, per attuare programmi di monitoraggio audit e test, per valutare la rilevanza dell'impatto di un incidente e segnalarlo all'autorità competente.

In Italia l'obbligo di notifica degli incidenti è stato recepito per entrambe le categorie di soggetti, rispettivamente con l'art.12 e l'art.14 del Decreto e si esplica attraverso:

- il Computer Security Incident Response Team - CSIRT[10] che, rispettivamente ciascuno Stato Membro dovrà istituire, ha il compito (art.9 della Direttiva) di trattare gli incidenti e i rischi secondo procedure ben definite
- l' Autorità competente NIS (per conoscenza) che, anch'essa unica per ciascuno Stato membro, ha il compito di controllare la corretta applicazione della Direttiva a livello nazionale.

Il CSIRT e il Punto di contatto unico

In Italia, con l'art.8 del Decreto, a partire dalla convergenza del CERT Nazionale e dal CERT PA, è stato costituito presso la Presidenza del Consiglio dei Ministri l'"*unico*" CSIRT italiano; anche in questo caso si attendeva entro il 9 novembre il rilascio di un provvedimento teso a definirne l'organizzazione. Purtroppo i tempi sembrano allungarsi, con un consequenziale impatto sull'operatività ed in particolare per la prevenzione e la risposta agli incidenti informatici.

Nota interessante tratta direttamente dal sito del CERT PA[11] è quella che afferma "*…nel frattempo, il CERT Nazionale e il CERT-PA, già operanti rispettivamente presso il Ministero dello Sviluppo Economico e l'Agenzia per l'Italia Digitale, rafforzano la loro pluriennale collaborazione per svolgere congiuntamente il ruolo e le funzioni del CSIRT Italiano. Il CERT Nazionale ed il CERT PA, nella fase transitoria, sulla base dell'esperienza maturata in questi anni, continuano a svolgere compiti di prevenzione e di risposta ad incidenti informatici, facilitando la mitigazione dei relativi effetti. In tale ottica, dall'entrata in vigore del D.Lgs. 65/2018, congiuntamente gestiscono le notifiche d'incidenti informatici, che nella fase transitoria hanno carattere obbligatorio solo per i fornitori di servizi digitali. Nell'attesa che le Autorità competenti NIS individuino gli operatori di servizi essenziali, le Imprese e le Pubbliche Amministrazioni – attive nei settori individuati dall'Allegato II della Direttiva – potranno su base volontaria segnalare eventuali incidenti informatici rispettivamente al CERT Nazionale e al CERT PA.*". In questa nota c'è un chiaro riferimento al già citato art.8 del Decreto e nello specifico a quanto previsto al comma 3; in tal senso il CERT Nazionale garantisce la cooperazione a livello europeo, anche nell'ambito della rete di CSIRT, in accordo con il CERT-PA.

Gli obblighi di notifica da parte del CSIRT Italiano ricomprendono nell'attuazione dell'intero processo, oltre che la comunicazione all'Autorità Competente anche la comunicazione al Punto di contatto unico, il DIS. Il ruolo focale di quest'ultimo si manifesta con il coordinamento generale di tutto ciò che concerne la sicurezza delle reti e dei sistemi informativi, la tutela dei rapporti (insieme alle Autorità Competenti) con le Autorità di contrasto e il Garante Privacy, e la salvaguardia della garanzia di cooperazione transfrontaliera a livello comunitario tra le Autorità Competenti italiane e le rispettive degli altri Stati Membri, il Gruppo di Cooperazione (con il quale tra l'altro ne partecipa alle attività) e la rete di CSIRT.

Tra i principali compiti del CSIRT italiano abbiamo la gestione degli incidenti notificati dagli operatori di servizi essenziali e i fornitori di servizi digitali e il coordinamento degli interventi tesi a contenerne l'impatto; ciò anche con la predisposizione e la divulgazione delle migliori procedure di gestione degli eventi e degli incidenti di sicurezza che devono ricomprendere aspetti metodologici di categorizzazione e classificazione, la gestione delle escalation nei confronti delle autorità di controllo, etc..

In tal senso le procedure di gestione degli incidenti di sicurezza devono essere predisposte tenendo conto la possibilità di dover procedere per lo stesso evento con una notifica verso più Autorità di Controllo - ad esempio al Garante Privacy in ottemperanza a quanto previsto dal GDPR, come pure alla Banca d'Italia quando ad essere coinvolti sono i servizi finanziari erogati dalle Banche.

Per la notifica degli incidenti, oltre alle disposizioni previste nel Decreto, si dovrà tener ulteriori risorse quali:

- il Regolamento di esecuzione (UE) 2018/151 della Commissione del 30 Gennaio 2018 che, per i fornitori di servizi digitali, individua tutti i parametri che consentono di determinare la rilevanza di un incidente e dunque la conseguente necessità o meno di procedere con la notifica nei confronti del CISRT Italiano;
- il sito del CSIRT italiano[12] dove nella sezione "Notifica incidenti" s'informa che la notifica dell'incidente deve essere effettuata utilizzando il modulo reso disponibile nella sezione "Modulistica" che, opportunamente compilato e cifrato con la chiave pubblica PGP[13] , deve essere inviato all'indirizzo notifica.nis@csirt-ita.it.

Al fine della valutazione dell'incidente, come si evince dal modulo di notifica del CSIRT e quindi al corretto coinvolgimento di tutti gli organi deputati alla collaborazione internazionale, si dovrà valutare l'impatto come fenomeno critico che interessa due o più Stati dell'Unione Europea. Tra l'altro il necessario coinvolgimento di due o più stati è un requisito stabilito dalla stessa Commissione Europea che, con il progetto "EPCIP"(European Program for Critical Infrastructure Protection), ha definito un sistema EU (ICE) che incardina la definizione di infrastruttura critica come: l'infrastruttura collocata negli stati membri dell'Unione Europea la cui distruzione o malfunzionamento avrebbe come conseguenza diretta un *impatto significativo* su almeno due Stati Membri dell'Unione.

Oltre alla gestione degli incidenti informatici, non meno importanti sono tutti quei servizi di sicurezza erogati dal CSIRT Italiano per favorire la cooperazione nazionale e internazionale, ad esempio partecipando alla rete dei CSIRT[14].

Tale rete è composta dai CSIRT degli Stati membri e da quello del CERT-UE (art. 11 del Decreto), e ha la funzione di garantire la migliore e costante condivisione d'informazioni in merito ad incidenti, schemi di attacco e minacce informatiche che ogni singolo Stato ha collezionato. Tra i vari servizi che operano nella medesima direzione, troviamo anche quelli per l'emissione di bollettini sulle vulnerabilità presenti nel software e nell'hardware dei sistemi informatici.

La strategia nazionale

Con l'art. 7 la Direttiva impone agli Stati membri di adottare una strategia nazionale con obiettivi, misure strategiche e regolamentari, inclusi i ruoli e le responsabilità degli organi istituzionali, per indirizzare aspetti di sicurezza delle reti e dei sistemi informativi, gestire gli incidenti informatici, sviluppare programmi di formazione e sensibilizzazione, favorire la collaborazione tra il pubblico e il privato, definire piani di ricerca e per la valutazione dei rischi.

L'Italia recepisce questo obbligo al capo II del Decreto in particolare fornendo una specifica elencazione all'art. 6 comma 2. Nell'ambito della definizione della strategia nazionale di sicurezza cibernetica è bene specificare i punti salienti che hanno caratterizzato l'evoluzione normativa.

Con D.P.C.M. del 24 gennaio 2013, il c.d. Decreto Monti, pubblicato sulla G.U. del 19 marzo 2013 n°66 si iniziava un processo particolarmente ambizioso per rendere efficiente il sistema di sicurezza nazionale in cyber security. Sempre nel 2013 fu istituito un Tavolo Tecnico Cyber (TTC) che portò alla stesura di due documenti: il *"Quadro Strategico nazionale per la sicurezza dello spazio cibernetico"*, integrato con il *"Piano Nazionale per la protezione cibernetica e la sicurezza informatica"* pubblicati nel mese di dicembre dello stesso anno. Tali documenti furono infine adottati con il comunicato D.P.C.M. del 27 gennaio 2014 poi pubblicato in Gazzetta Ufficiale il 19 febbraio 2014, n. 41.

Rimanendo sostanzialmente invariata la strategia, comunque da rivedere per cogliere nella sua interezza quanto previsto nell'art.7 della Direttiva , con il D.P.C.M. del 17 febbraio 2017 è stata aggiornata la direttiva recante gli indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, adottando con il D.P.C.M. del 31 marzo 2017 quello che è il nuovo *Piano nazionale per la protezione cibernetica e la sicurezza informatica nazionali.*

Il *Quadro Strategico nazionale per la sicurezza dello spazio cibernetico* nel concreto si articola in sei indirizzi strategici: il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese, il miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati, l'incentivazione della cooperazione tra istituzioni ed imprese nazionali, la promozione e diffusione della cultura della sicurezza cibernetica, il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica e il rafforzamento delle capacità di contrasto alle attività e contenuti illegali on-line. Con il secondo documento il *"Piano Nazionale per la protezione cibernetica e la sicurezza informatica"* sono invece fissati gli indirizzi operativi per conseguire quelli strategici.Gli indirizzi operativi riguardano più specificatamente: il potenziamento delle capacità d'intelligence, di polizia e di difesa civile e militare,il potenziamento dell'organizzazione e delle modalità di coordinamento e d'interazione a livello nazionale tra soggetti pubblici e privati, la promozione e la diffusione della cultura della sicurezza informatica, la formazione e l'addestramento, la cooperazione internazionale e le esercitazioni, l'operatività delle strutture nazionali per la gestione degli incidenti, gli interventi legislativi e di compliance rispetto agli obblighi internazionali, la compliance a standard e protocolli di sicurezza, il supporto allo sviluppo industriale e tecnologico, la comunicazione strategica e operativa, le risorse e l'implementazione di un sistema di cyber risk management nazionale.

Conclusioni

Le sfide che la Comunità Europea e gli Stati membri stanno affrontando in questo delicato e alquanto complesso comparto, sia da un punto di vista tecnologico, sia da un punto di vista dell'adeguamento normativo, richiedono grandi sforzi e un cambio culturale che deve basarsi sempre di più su aspetti d'innovazione resi possibili "in primis" con la ricerca e lo sviluppo, una maggiore disponibilità di d'investimenti (mentre Israele investe circa il 4% del proprio PIL in ricerca e sviluppo, l'Italia investe appena l'1,3%[15]) e strumenti d'incentivazione, lo sviluppo delle competenze, la valorizzazione del capitale umano e molto altro ancora (es. campagne di sensibilizzazione, etc.). A titolo meramente esemplificativo, la ricerca e lo sviluppo dovrebbero essere parte integrante di un programma orientato ad innalzare il livello di sicurezza del sistema paese, con una cabina di regia al comando in grado di indicare l'orientamento alle imprese pubbliche e private, nonché le tempistiche, il tutto per valorizzare gli investimenti fatti e infondere la percezione che la sicurezza non è solamente un costo ma un reale valore da tutelare. ■

1 https://www.repubblica.it/tecnologia/sicurezza/2018/02/21/news/l_anno_vissuto_pericolosamente_dall_italia_11_milioni_di_nostri_account_in_vendita_sul_dark_web-189425514/ Basti pensare che in Italia
2 https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
3 http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643
4 http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53644
5 http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53645
6 http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646
7 http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53677
8 http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53675
9 http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53661
10 ENISA definisce il CSIRT "è un gruppo di esperti in sicurezza IT, la cui attività principale consiste nel reagire a incidenti di sicurezza informatica. Esso fornisce i servizi necessari per affrontare tali incidenti e aiutare i relativi utenti di riferimento a riprendersi dalle violazioni. Al fine di attenuare i rischi e ridurre al minimo il numero d'interventi richiesti, la maggior parte dei CSIRT fornisce anche servizi preventivi e didattici per la propria comunità di riferimento. Essi emettono bollettini informativi sulle vulnerabilità presenti nei software e hardware in uso e informano gli utenti in merito agli exploit (attacchi finalizzati a produrre accesso a un sistema o incrementi di privilegio) e ai virus che approfittano di queste debolezze. Gli utenti di riferimento possono quindi porvi rapidamente rimedio e aggiornare i loro sistemi.", Un approccio graduale alla creazione di uno CSIRT.
11 https://www.cert-pa.it/csirt-italiano/
12 https://www.csirt-ita.it/
13 Chiave pubblica PGP del CSIRT Italiano: 2960 3E4EA7148C12227BCA4AE42790DDA969D6EC
14 Il primo incontro formale della rete dei CSIRT si è svolto a Malta tra il 22 e il 23 febbraio 2017. L'incontro è stato organizzato da CSIRTMalta in collaborazione con l'ENISA nell'ambito della presidenza maltese del Consiglio del Unione Europea (gennaio - giugno 2017), promovendo per il conseguimento degli obiettivi a breve termine previsti nei successivi 18 mesi (da febbraio 2017 ad agosto 2018) la formazione dei seguenti gruppi di lavoro:WG1: test del portale ENISA, WG2: livello di maturità, WG3: requisiti specifici per i servizi operativi, WG4: SOP e WG5: comunicazioni con il gruppo di cooperazione.
15 Corriere della Sera, mercoledì 14 novembre 2018

Nell'ambito della sicurezza le aziende sono la prima linea di difesa

Intervista VIP a Luciano Floridi

Luciano Floridi

Autore: Massimiliano Cannata

Luciano Floridi è una delle voci più autorevoli della filosofia contemporanea. Professore ordinario di filosofia ed Etica dell'informazione all'Università di Oxford, dirige il *Digital Ethics Lab* ed è *chairman* del *Data Ethics Group dell'Alan Turing Institute*. Lo abbiamo raggiunto al telefono, in un breve pausa tra una conferenza e l'altra, per cercare di capire qualcosa in più sulla rivoluzione digitale che sempre più prende le nostre vite.

Professore, nel suo saggio* La quarta rivoluzione *(Raffaello Cortina) un capitolo è dedicato al rischio digitale, vorrei partire da questo aspetto. Come si può sviluppare una* governance *della sicurezza adeguata, proteggendo le reti e difendendosi dallo strapotere degli algoritmi, che molti pensatori definiscono "Datacrazia"?

Siamo a un cambio di paradigma e continuiamo a gestire il rischio come se fossimo ancora nella società industriale, senza comprendere che il rischio va affrontato servendosi delle banche dati, dell'infinita capacità di processare le informazioni. Strumenti come il software intelligente ci permettono di prevedere e calcolare le possibili vulnerabilità e di fare un lavoro di prevenzione fino a ieri impensabile. Il digitale è, insomma, un ausilio dirompente per la security. Direi di più: il bicchiere di questa rivoluzione è per due terzi pieno e per un terzo vuoto proprio in ragione delle potenzialità di una migliore gestione del rischio di cui disponiamo grazie al digitale.

Le aziende che compito hanno sul fronte della sicurezza?

Enorme, sono la prima linea di difesa, non scordiamolo. Una forza dirompente come il digitale presenterà pure delle criticità, ma anche immensi margini di sviluppo, a patto di saper sfruttare e di conoscere i nuovi

BIO

Professore di Filosofia ed Etica dell'informazione all'Università di Oxford, dirige il Digital Ethics Lab dell'Oxford Internet Institute, il Data Ethics Research Group dell'Istituto Alan Turing e il comitato consultivo sull'etica dell'European Medical Information Framework. Esperto di filosofia dell'informazione – disciplina di cui è considerato il fondatore -, di computer ethics, data ethics, di etica dell'informazione e di filosofia della tecnologia, è anche membro del comitato consultivo di Google sul "diritto all'oblio". Con la Oxford University Press ha pubblicato, tra gli altri, *The Fourth Revolution* (2014), *The Ethics of Information* (2013), *The Philosophy of Information* (2011). La sua ultima pubblicazione in italiano: La rivoluzione dell'informazione (Codice 2012). È in corso di stampa presso Raffaello Cortina, *La Quarta Rivoluzione. Come l'infosfera sta trasformando il mondo (2017).*

linguaggi. Quando vedo paura dei robot e delle macchine intelligenti penso: è pura fantascienza! Piuttosto incamminiamoci dentro l'"infosfera", che sta cambiando non solo noi stessi, ma il mondo in cui ci muoviamo nel mondo.

Una definizione di infosfera. A proposito: "infosfera" è un termine che ha coniato e che sta riscuotendo successo e interesse. Possiamo spiegare di che si tratta?

Abbiamo in passato sempre trattato le tecnologie di cui disponiamo come dei semplici canali di comunicazione. E' stato così per il telefono, la televisione, la radio. Oggi, però, siamo di fronte a un salto di qualità. Gli apparati digitali creano un ambiente. Prima si stava al telefono, oggi si vive su Internet, si guardava la tv, assistendo a uno spettacolo, oggi siamo protagonisti di quello spettacolo. Lo spazio dentro cui viviamo è fatto di informazione, siamo in un ambiente dove si mescolano in modo inestricabile analogico e digitale, on line e off line, è questa l'infosfera.

La stessa telefonata che lei mi ha fatto a Oxford è fondata su questo mix: mentre parliamo, il telefonino mantiene la nostra geolocalizzazione, inviando continuamente informazioni a una centrale che rielabora dati su dati.

Il "Reale" e il "virtuale" si incrociano. Appare ormai superata la visione di Pierre Levy, il primo pensatore che aveva messo a confronto queste categorie. Si apre un nuovo percorso per la riflessione filosofica e scientifica?

Si tratta di rivedere proprio le categorie dell'essere che per una certa parte della nostra storia abbiamo fondato sulle cose che possiamo toccare, vedere, sentire. Quando è arrivata la dimensione del virtuale abbiamo cominciato a superare le forme ingenue dell'empirismo. Abbiamo per dirla in sintesi capito che non contano solo gli oggetti le cose che possiamo volgarmente "prendere a calci", perché una grandissima parte dell'universo è fatto di energia, di campi di forze, di flussi.

Un cambiamento non da poco?

Uno stravolgimento di prospettiva, perché il criterio di esistenza non è solo quello percettivo, ma interattivo. In altri termini vuol dire che se con qualcosa posso interagire, quel qualcosa esiste. L'icona del PC esiste, la posso "cliccare". Essere cliccabile nella società del web vuol dire esistere. Diventa questo il criterio per certificare l'esistenza di un ente è, infatti, crollata la vecchia distinzione tra reale e virtuale tutto è rimescolato, le vecchie categorie della speculazione non bastano a spiegare la complessità entro cui siamo immersi.

Realismo e idealismo sono sottosopra. In che mondo viviamo allora?

A seconda delle capacità di interazioni viviamo in mondi con "ontologie" diverse, chi può avere interazioni con un mondo molto più ricco, più ampio e diversificato, vive "meglio" rispetto a chi si trova in realtà chiuse, isolate, che sono fatalmente più povere, meno stimolanti. In passato la distinzione era imperniata sui diversi mondi linguistici, il mio mondo e il mio linguaggio, sostenevano autorevoli pensatori. Si trattava di una concezione semantica, che metteva in primo piano il problema della traducibilità, senza di cui non ci poteva essere comunicazione, né relazione, né dialogo tra gli individui. Adesso invece si deve puntare la ricerca sull'interazione, che diventa la chiave attorno a cui conoscere la realtà e far crescere competenze ed esperienze.

Dall'industriale al digitale. Facciamo atterrare questo interessante ragionamento filosofico. Quali sono le ricadute tecnico - economiche ed etico - sociali legate al passaggio dall'industriale al digitale?

La *sharing economy*, modello di business sempre più praticato è una diretta conseguenza del passaggio al nuovo paradigma digitale. Il nuovo capitalismo impone, a differenza del passato, la condivisione, in quanto strumento che rende più forti e ricchi i soggetti imprenditoriali e gli stessi individui.

L'economia circolare è l'altro tassello su cui bisogna insistere, in questo caso non si tratta di una novità, ma di un ritorno. I nostri nonni non buttavamo niente, vivevano nella società agricola, che valorizzava il risparmio e l'utilizzo completo delle poche cose di cui si disponeva. Quando si affermata poi l'economia lineare. A seguito della prima rivoluzione industriale, l'unica cosa importante è diventata l'acquisizione di cose e di oggetti per liberarsene subito dopo, cessata la necessità d'suo. Oggi stiamo tornando a una "circolarità acquisita", non più povera come nel vecchio schema, ma affluente.

In concreto?

Significa che il digitale rende possibile le modalità di un'economia circolare affluente, in quanto permette di economizzare, riutilizzare, utilizzare meglio, fare di più avendo meno. Sostenere che la tecnologia è nemica della natura è un errore, è un giudizio risultante di

un vecchio retaggio ancorato al primo passaggio storico dall'economia circolare all'economia lineare. L'innovazione di questa "quarta ondata" per parafrasare *Alvin Toffler* (che parlava in un noto saggio di "Terza ondata" n.d.r.) ci sta portando verso il nuovo orizzonte di un'economia circolare *verde e affluente*, che vede per la prima volta tecnologia e natura alleati.

In un'intervista recente Diego Piacentini, ex Commissario straordinario per l'attuazione dell'agenda digitale, facendo un bilancio del suo mandato ha detto: un'impresa affrontare il cambiamento nella PA, ci sarà da lavorare ancora molto. Lei gira il mondo in lungo e in largo. Come siamo messi in Italia?

Dal punto di vista tecnico – infrastrutturale passi avanti ne abbiamo fatti. Stiamo recuperando un gap storico, in un paio di anni penso che saremo vicini agli altri paesi europei. La banda larga esiste, i pagamenti on line vengono effettuati, la connessione è disponibile in tutto il territorio. E' la mentalità digitale che dobbiamo acquisire. Dobbiamo imparare a pensare più in termini di interazione, che di percezione. Il nostro cervello di mammiferi ci porta a vedere un mondo fatto di cose, quello che contano sono gli oggetti e le loro proprietà, quando invece dovremo vedere il mondo in termini di interazione, ricordandoci che le cose vengono dopo, ci sono prima le relazioni e i processi. La fisica lo sa molto bene da molto tempo. Sono i campi di forza dove i processi si incrociano che devono destare, insomma, il nostro interesse.

Possiamo fare un esempio per intenderci?

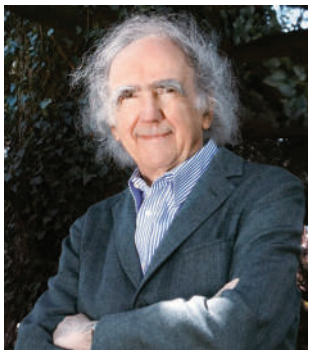
Utilizzo un'immagine di cui mi sono servito a Milano in un convegno in sui abbiamo discusso di innovazione: le rotonde arrivano prima delle strade? Ovviamente no, sono prima le strade che si sviluppano in certe direzioni e si incrociano. Le rotonde vengono pensate e costruite dopo. Dobbiamo capovolgere il punto di vista: prima ci sono processi e relazioni, poi arrivano gli oggetti. Se ci riflettiamo bene anche la sedia su cui poggiamo è un agglomerato di processi e relazioni.

Verso un capitalismo inclusivo. In conclusione professore se dovesse suggerire da dove ripartire. Cosa si sente di dire?

Dalla prospettiva di un capitalismo inclusivo capace di puntare sugli alfabeti digitali per migliorare la qualità della vita e del lavoro. Solo a queste condizioni si potrà compiere una "migrazione virtuosa" dallo spazio fisico newtoniano al nuovo orizzonte immateriale, edificato sulla condivisione di saperi, idee e informazioni. Questo particolare "serbatoio", che come dicevo all'inizio, chiamo "infosfera", non è altro che un immenso patrimonio da spendere al servizio della convivenza pacifica e del progresso, uno spazio comune che va preservato a vantaggio di tutti. ■

Da *"sapiens"* a *"stupidus"*: se trascuriamo valori la civilta' tecnologica rischia di precipitare nella barbarie

Intervista VIP a Vittorino Andreoli



Vittorino Andreoli

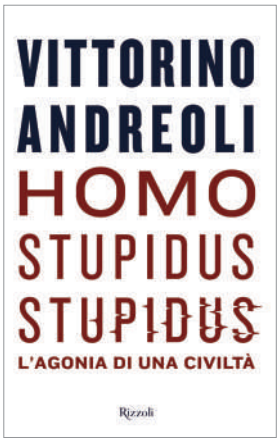
Autore: Massimiliano Cannata

«Non stiamo dando più importanza ai principi con il risultato che stiamo progressivamente precipitando nella barbarie. La civiltà non è un fatto scontato, ma una conquista che passa attraverso la trasmissione di valori e comportamenti. Così da *sapiens sapiens*, l'uomo di oggi corre il rischio di trasformarsi in *"stupidus stupidus"*, facile preda di nuove solitudini oltre che vittima di una patologia sempre più diffusa: *l'autismo digitale*».

Fa molto riflettere l'ultimo saggio di Vittorino Andreoli, *(Homo Stupidus Stupidus, edito da Rizzoli)* tra i più noti psichiatri italiani, da sempre attento osservatore e studioso delle complesse dinamiche sociali che attraversano la contemporaneità.

Professore, come Lei scrive l'uomo sembra aver perso il "beneficio della neocorteccia". Perché la nostra specie sta facendo di tutto per "meritare" il poco lusinghiero attributo di "Stupidus Stupidus"?

Dobbiamo prima di tutto intenderci su un dato di fondo: la civiltà che abbiamo faticosamente raggiunto nel corso di millenni di storia si fonda su principi e comportamenti praticati e appresi. Significa che se non riusciremo a trasmettere alla prossima generazione determinati valori e stili di comportamento, siamo destinati a smarrire tutto quello che abbiamo erroneamente considerato come un patrimonio definitivamente acquisito. Le neuroscienze sono molto chiare in proposito.



Cosa intende dire?

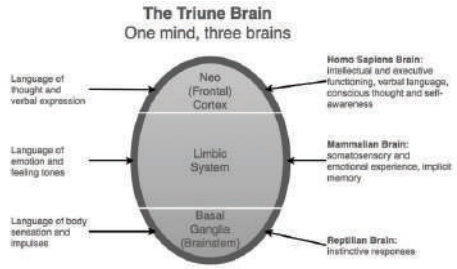
Semplicemente che il grado di civiltà che abbiamo conquistato con grande sforzo, non è contenuto nei nostri geni, non è la realizzazione dovuta alla messa in pratica di un comportamento meccanico istintuale, è un importante risultato propiziato da quella parte del cervello "plastico" che si forma sulla base delle esperienze e che presiede all'apprendimento, alla creatività, che è poi il vero motore della nostra attività intellettuale. Vuol dire in concreto che i neuroni di questa porzione della neocorteccia si riuniscono in circuiti, in una struttura sofisticata che presiede al tatto mnemonico, all'idea, alle facoltà cosiddette superiori. Così se non diamo più importanza alla dimensione valoriale e ai principi, al rispetto della vita, la regressione diventa, non un'ipotesi vaga, ma un prospettiva certa.

BIO

Vittorino Andreoli, psichiatra di fama mondiale, è stato direttore del Dipartimento di Psichiatria di Verona - Soave ed è membro della New York Academy of Sciences. Ha pubblicato decine di saggi. Tra le sue ultime opere pubblicate possiamo citare «Le nostre paure» (2011), «Elogio dell'errore» (2012, con Giancarlo Provasi), «Il denaro in testa» (2012), «L'educazione (im)possibile» (2014) e il recentissimo «Homo Stupidus Stupidus»

Ripiombare nella barbarie, come ha denunciato Alessandro Baricco nel suo celebra saggio "I barbari", da provocazione diventa un fatto possibile?

Mi permetta una citazione. Il neuroscienziato *Paul Donald MacLean* sostiene che abbiamo tre cervelli. Il primo è quello degli istinti, proprio dei rettili, il secondo è quello delle emozioni, posseduto dai mammiferi, il terzo è quello del pensiero inteso in senso più alto. Sappiamo grazie agli studi più recenti che mentre i primi due sono stampati e prefigurati fin dalla nascita, come si trattasse di un PC che ha già il software definito, il terzo si forma dentro di noi, come risultato di un processo. Le scoperte eccezionali operate dall'uomo sono frutto di un'evoluzione continua, è questa la nostra grandezza, ma anche la nostra debolezza, perché non si tratta di un percorso irreversibile, il pericolo che si inneschi una marcia indietro è sempre dietro l'angolo. Le criticità emergono nel momento in cui, come dimostrano i tanti casi di attualità, si fa strada la mancanza di rispetto dell'altro e i valori vengono calpestati, a quel punto a dominare non sarà più il cervello alto ma quello basso, quello che presiede i bassi istinti. E' così che si piomba in quella che Gianbattista Vico definiva: la "condizione selvaggia". Ognuno tenderà ad appropriarsi di tutto ciò che vuole, i tanti femminicidi praticati per cieca gelosia, la violenza sui bambini e gli esseri più indifesi dimostrano che non ci sono più regole, l'altro è un nemico da abbattere. Possiamo definire *"sapiens sapiens"* un'umanità ridotta in questo stato?



La tecnologia, questa protesi che dovrebbe colmare la nostra imperfezione, che ha generato una sorta di pericolo "illusionismo" è la principale responsabile di questa marcia indietro?

La tecnologia, penso per esempio allo sviluppo del cervello digitale, ha permesso grandi conquiste. Senza il PC non avremmo scoperto il bosone di *Higgs*, le onde gravitazionali, ingegneri e fisici ormai costituiscono il corpus di un'intelligenza collettiva che ci porterà a nuovi traguardi. Il problema nasce quando si fa un uso distorto di questi strumenti. Faccio un esempio: stiamo perdendo l'uso della memoria dei numeri. Per telefonare a un amico o a un genitore facciamo un clic, senza fare nessun esercizio per ricordare il numero. Questo vuol dire che fra non molto non sapremo fare più alcun calcolo, il mondo dei numeri di fatto è scomparso. Discorso ancora più grave si può fare per la memoria semantica. Quando parliamo siamo abituati ad associare un suono a un significato. Nel linguaggio ordinario usiamo circa 150 parole, poche rispetto alle trentamila indicate dalla Treccani, questo declino già denunciato dai linguisti è destinato ad accentuarsi, perché la maggior parte delle persone comunicano con dei segnali, utilizzando il pc. Il rischio che si profila è quello di non parlare più, arriveremo all'AUTISMO DIGITALE, un universo chiuso, popolato da tante monadi che non comunicano. Il Pc rafforza questa tendenza alla schematizzazione: utilizziamo il ditino in su se qualcosa piace e in giù quando non piace. A dominare è la logica binaria, non più la logica razionale che, almeno da Aristotele in poi, è posta a fondamento del pensiero e della civiltà occidentale.

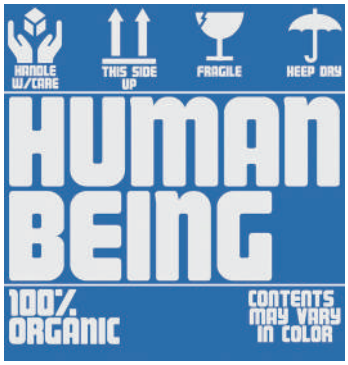
Le "costanti di distruttività". Oltre alla progressiva "caduta dei principi" il saggio denuncia l'escalation di alcuni fattori "costanti di distruttività", quali: violenza, guerre, volontà di difesa del territorio. Si tratta di elementi che da sempre caratterizzano la specie umana, in perenne lotta per la sopravvivenza. Oggi la posta in palio è però ancora più alta: l'intera civiltà occidentale sta correndo verso il baratro. Cosa possiamo fare?

Il rischio esiste e va denunciato. Non sono un apocalittico, ci sarà sempre l'uomo a emergere, in altri contesti storico geografici si stanno facendo infatti strada i filosofi del post human, che apriranno nuovi spiragli di pensiero di riflessione. E' la civiltà occidentale sotto scacco se non riusciamo a trovare adeguate contromisure. La questione non è tanto relativa alla violenza, che è un comportamento orientato a uno scopo, e in quanto tale si può ridimensionare e sconfiggere. La distruttività mi preoccupa molto di più, quella cieca volontà di potenza che travolge tutto, il terrorismo globale è l'esempio drammatico che può far comprendere a cosa mi riferisco. Tutto viene travolto senza un fine, il corpo diventa un'arma, che ingoia tutto. Così abbiamo distrutto antiche città, musei, luoghi di ritrovo, biblioteche. Difficile trovare un antidoto di fronte a una follia, che non ha più una logica, un orizzonte di senso.

Il potere, tra i fattori di distruttività elencati, è forse il termine più ambivalente. Come lo si può definire nel contesto della società globale che sta sperimentando una profonda mutazione del concetto stesso di democrazia?

Quando parlo del potere intendo il potere come "verbo" perché il sostantivo include il concetto di autorità, divenendo altro e va maneggiato con cura. Potere come verbo vuol dire: faccio perché posso. Come nel caso che ricordavo della distruttività, esiste anche un potere che viene esercitato senza scopo. Platone sosteneva che il potere doveva avere come fine supremo la felicità di tutti. Oggi non accade nulla di tutto questo: la dinamica la si vede molto bene anche nella politica, dove spesso si contraddice l'altro solo per spirito di propaganda senza mai entrare nel merito delle questioni. Il Potere fine a se stesso è, insomma, il "verbo dominante" di questa epoca densa di contraddizioni.

La condizione dell'uomo contemporaneo, incerto e confuso, non comprende più il potere, sembra solo subirlo, non crede?



La condizione umana si caratterizza per la fragilità, che è data dal bisogno dell'altro, dal desiderio di conoscere, mentre il potere non ha bisogno dell'altro se non per dominarlo. Questo è l'umanesimo della fragilità, che segna e segnerà le nostre vite.

La rete e i "padroni dell'umanità". ***Malgrado tutto l'individuo è capace di risollevarsi. L'"uomo rotto", spiega nel saggio, può ritrovare la serenità. Dobbiamo essere ottimisti?***

Mi definisco un "pessimista attivo". I rischi sono quelli che abbiamo cercato di individuare, ma bisogna continuare a cercare il meglio senza sosta. Nel lungo cammino della nostra evoluzione abbiamo meritato il doppio appellativo di "sapiens", se pensiamo alla poesia, al Canto XXXIII del Paradiso, alla scienza, alle grandi scoperte ci ricordiamo di quante meravigliose realizzazioni l'uomo è stato ed è capace. Dietro "l'uomo rotto", che ho studiato con massimo interesse da psichiatra, ho sempre ritrovato questa grandezza di cui ogni individuo è portatore, per questo continuo a guardare avanti con fiducia.

"Neoumanesimo digitale" è la prospettiva da più parti auspicata, come ci ricordano gli ultimi scritti di Morin, Sennett, Ceruti, Sen, e dello stesso Baricco ricordato prima. Le pare una via d'uscita realmente praticabile?

A condizione di tornare a un umanesimo nuovo, che guardi all'altro come valore, dove ci sia un senso del limite, che bandisca quella stupidità, che non conosce la sapienza. Lo stupido si ritiene perfetto, il sapiente coltiva il dubbio, per questo ha dei margini di crescita. Tutta la nostra civiltà è fondata sul dubbio, i dialoghi di Platone, hanno questa radice che è la stessa che informa l'*"umiltà socratica"*. Difendiamo ciò che umano. Non vergognandoci di quella fragilità che mi porta ad avere bisogno dell'altro, nella consapevolezza di quell'utilità reciproca, che rinsalda il bisogno della relazione e del confronto.

Avremmo in sintesi bisogno di riaffermare la centralità di un individuo più equilibrato, non certo un "uomo senza misura" che vive il capovolgimento della dimensione Protagorea, che vedeva il soggetto come espressione di una suprema armonia tra spirito e natura. Riusciremo a recuperare il giusto bilanciamento in una società sempre più polarizzata, rosa da povertà crescenti, preda di paure e di una crescete insicurezza?

Potremo riuscirci se ci impegneremo a scrollarci di dosso la duplice attribuzione di *"stupidus", "studidus"*. Utilizzo ancora questo termine nel senso di stupore, perché rimango attonito nel constatare come l'uomo possa precipitare così in basso, dopo esser stato protagonista di tante straordinarie conquiste. Purtroppo abbiamo perso la misura. Torno a parlare delle tecnologie e del loro uso. Internet è un eccezionale strumento, purtroppo oggi è sempre più in mano di poche persone, che non sono imprenditori ma sfruttatori. Il linguista Noam Chomsky li ha in un recente saggio definiti *"I padroni dell'umanità"*, si tratta di individui senza scrupoli che si prendono gioco dell'uomo, per questo entrano nelle loro vite, violano la *privacy*, senza ritegno alcuno. Il recente caso di *Cambridge Analytica* deve far riflettere chi opera sul fronte della sicurezza dei dati.

Valori e società digitale ***La tendenza a semplificare fa sì che non si problematizzano più parole come "Verità", "Religione", "Bellezza", "Res Publica", "Amicizia", "Ragione", termini complessi che hanno impegnato per secoli scienziati e filosofi. Il "pensiero dominante" sembra avere tutto l'interesse a semplificare negando la densità e la profondità di un tessuto concettuale, che appartiene alla nostra storia e civiltà. Quali sono le ragioni di questo atteggiamento?***

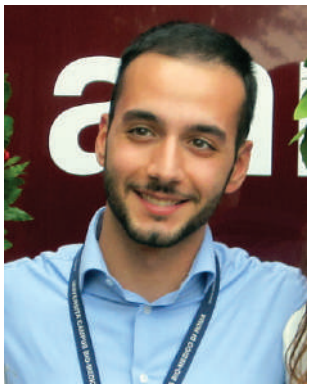
E' una tendenza diffusa che mira al pensiero unico, a negare la differenza e il pluralismo. Pensiamo alla religione. Al di là delle diverse confessioni, rammentiamoci che un Dio esiste per tutti, perché esiste un'impronta del sacro. Sappiamo tutto questo ma ci fermiamo a commentare solo piccoli fatti, segnati da esteriore superficialità. Eppure il sentimento religioso fa parte dell'essenza dell'uomo. Solo gli individui concepiscono la trascendenza, percepiscono una verticalità, che gli scimpanzé non possono né sentire, né concepire.

In chiusura del saggio evoca "Timore e tremore", celebre opera del grande filosofo danese Soren Kierkegaard. Che cosa fa tremare e cosa terrorizza uno psichiatra che ha saputo, nel corso di una lunga e brillante carriera, misurarsi con tante manifestazione del male, esorcizzandolo?

Misurarsi con la dimensione dell'assurdo. Quello che descrive Kierkgaard in *"Timore e tremore"* è degno di studio per l'uomo di ogni tempo. Dio, come è noto, suggerisce

ad Abramo di sacrificare il figlio Isacco. Un controsenso, qualche cosa di inaccettabile per qualsiasi genitore. Abramo riesce comunque a trovare una soluzione, va oltre l'assurdo, segue la regola che ha appreso: sa che Dio c'è, ne ha avuto esperienza. Noi di fronte alle contraddizioni che attanagliano l'uomo contemporaneo a differenza di Abramo non facciamo niente, scappiamo. Il grande conflitto, il dramma è proprio questo: c'è una strada indicata dalla civiltà che ci porta verso l'alto, all'opposto ne esiste un'altra che ci porta verso la regressione. Non dobbiamo mai finire di lottare entrare dentro questa contraddizione per superarla, perché a prevalere sia la tensione verso obiettivi di progresso e di crescita umana e civile, perché di questo, mi creda, abbiamo un bisogno estremo e disperato. ■

Resilienza ed Infrastrutture Critiche: un nuovo approccio per l'allocazione delle risorse



Autore: Luca Faramondi

Una delle maggiori sfide nella gestione della sicurezza delle infrastrutture critiche è l'individuazione di una politica di allocazione ottimale delle "scarse" risorse per la loro protezione al fine di garantire adeguati livelli di sicurezza e resilienza. In questo contesto, un passo fondamentale è la corretta individuazione di quegli elementi e/o parti dell'infrastruttura che sono maggiormente critici per l'erogazione dei diversi servizi.

Spesso, in ambito scientifico, la ricerca delle criticità di una infrastruttura è superficialmente ridotta alla ricerca di quei nodi della rete che rappresentano gli hub, cioè nodi centrali dal punto di vista topologico e geografico e fortemente connessi con gli altri nodi della rete.

La metodologia proposta in questo articolo vuole riassumere l'approccio studiato presso il laboratorio di sistemi complessi e sicurezza dell'Università Campus Bio-Medico di Roma, che ha come obiettivo l'identificazione di quei nodi di una infrastruttura considerati fondamentali al fine di garantire la connettività tra ogni nodo della rete.

L'approccio applicato dal gruppo di ricerca è basato sull'assunzione della prospettiva di un attaccante, interessato alla distruzione di una rete, il cui comportamento può essere descritto da due regole fondamentali: eseguire un attacco il meno costoso possibile (in termini economici e di risorse impiegate) e massimizzare il danno arrecato all'infrastruttura.

Il problema da risolvere è dunque evidentemente un problema con due obiettivi contrastanti: all'aumentare del costo dell'attacco aumenteranno anche gli effetti negativi dell'attacco, mentre al diminuire delle risorse impiegate diminuiranno i danni arrecati alla rete. Quindi la strategia dell'attaccante si può ricondurre, per semplicità, alla ricerca di quelle azioni di attacco (ovvero target da attaccare) che garantiscano un buon rapporto tra costo dell'azione malevola e danno arrecato all'infrastruttura.

Tale tipologia di problemi è frequentemente affrontata nel contesto della ricerca operativa ed è identificata come *Multi-Objective Optimization Problem*. Una caratteristica di questa classe di problemi è che, in genere, esistono più soluzioni "ottimali", ognuna caratterizzata da un costo più o meno elevato ed un impatto sulla rete più o meno considerevole. Sostanzialmente, quindi, un attaccante ha una moltitudine di possibili target ottimali individuati in funzione della sua propensione ad "investire" risorse nell'attacco ovvero del suo "desiderio" di ottenere un danno elevato nell'infrastruttura.

Negli schemi classici di analisi il difensore, non avendo indicazioni puntuali su quella che sarà la strategia che metterà in atto l'attaccante, effettuerà una valutazione dei possibili target da proteggere sula base di ipotesi (leggi profilazione) su ciò che farà l'attaccante.

Questa soluzione ha però il grosso limite che, qualora le ipotesi sulla strategia che l'attaccante metterà in piedi siano errate, si allochino in modo non adeguato le risorse. In altri termini, nonostante il significativo investimento di risorse nella protezione, l'infrastruttura è ancora molto vulnerabile.

L'analisi che abbiamo proposto cerca di superare questa limitazione. Per fare questo il nostro approccio cerca di considerare, con una visione olistica, tutte le

BIO

Luca Faramondi ricopre attualmente il ruolo di assegnista di ricerca presso il laboratorio "Complex Systems & Security Lab" dell'Università Campus Bio-Medico di Roma ed è docente a contratto del corso di Sistemi di Controllo per l'Automazione Industriale presso l'Università di Cassino e del Lazio Meridionale. L'attività di ricerca riguarda la protezione cyber e fisica delle infrastrutture critiche. Nel 2018 ha vinto il secondo premio del "CIPRNet Young Critis Award, un riconoscimento conferito ai ricercatori sotto i 32 anni che si sono distinti per i loro studi nel campo della sicurezza delle infrastrutture critiche. Dal 2017 è membro dell'IEEE SMC Technical Committee on Homeland Security.

possibili strategie di attacco ottimale. Da un punto di vista matematico, questo vuole dire, considerare tutte le soluzioni ottimali al problema multi obiettivo, ovvero quello che è definito come fronte di Pareto.

L'analisi effettuata terrà quindi in considerazione profili differenti di ipotetici attaccanti con capacità economiche più o meno significative ma sempre interessati al massimizzare il danno arrecato all'infrastruttura con gli strumenti di cui dispongono. In questo modo, l'approccio presentato non vincola in alcun modo, ne suppone a priori, la conoscenza della strategia di attacco se non l'intento di massimizzare il danno arrecato.

L'analisi che proponiamo si basa sulla frequenza con cui ogni nodo della rete risulta coinvolto in differenti piani di attacco nonostante i costi e gli effetti differenti. Tale metrica è stata definita come "indice di criticità del nodo".

L'analisi della distribuzione dei valori della metrica appena definita, ha permesso di identificare i nodi più critici, ovvero più attrattivi dal punto di vista di un attaccante.

Si noti che per poter applicare tale schema di analisi delle vulnerabilità, è necessario quantificare il danno arrecato alla rete nel momento in cui un nodo smette di funzionare perché considerato sotto attacco. Nello specifico, la nostra soluzione suggerisce di definire il danno arrecato in termini di degrado apportato alla connettività della rete nel momento in cui tale elemento smette di funzionare. Il concetto di connettività nel contesto cyber può essere generalizzato e riletto in ottica di collegamento tra due nodi.

L'idea di utilizzare la connettività come indice di impatto dell'attacco sulla rete deriva dal fatto che riteniamo tale caratteristica fondamentale per il funzionamento di una rete di telecomunicazione. In ogni caso l'approccio proposto è personalizzabile definendo nuove misure che descrivano l'effetto dell'attacco sulla rete.

Dal punto di vista matematico, la connettività è espressa in termini di "pairwise connectivity" la quale corrisponde al numero di nodi della rete connessi tra loro mediante un cammino (ovvero un collegamento).

L'obiettivo dell'attaccante, dunque, sarà quello di "spezzare" la rete in più partizioni al fine di non rendere fruibili i servizi che la caratterizzano o rendendo impossibile il raggiungimento di un nodo (server) da parte di un altro nodo (client).

Partendo da questa formulazione, l'azione dell'attaccante e il suo piano di attacco sono modellati come la rimozione di un sottoinsieme di nodi dalla rete con l'obiettivo di minimizzare la connettività con il minimo sforzo economico ed impiego di risorse.

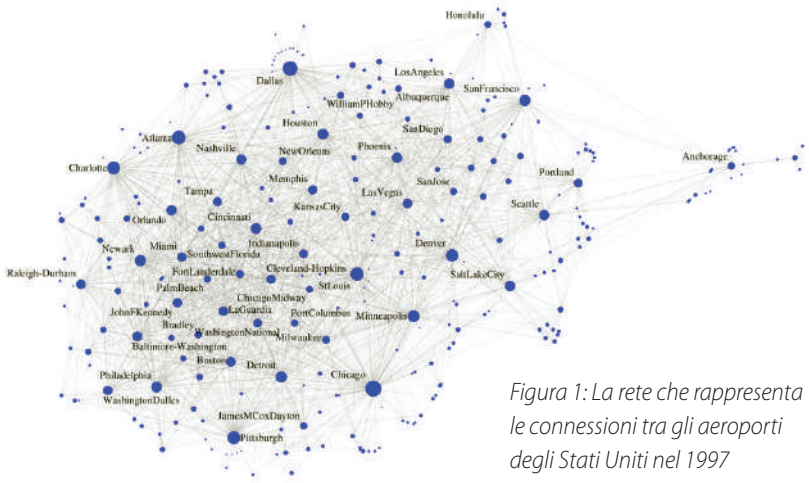


Figura 1: La rete che rappresenta le connessioni tra gli aeroporti degli Stati Uniti nel 1997

All'interno dello stesso studio, al fine di considerare uno scenario più realistico possibile, sono stati anche considerati aspetti legati all'eterogeneità dei nodi della rete e del costo necessario per coinvolgere quest'ultimi in un attacco malevolo.

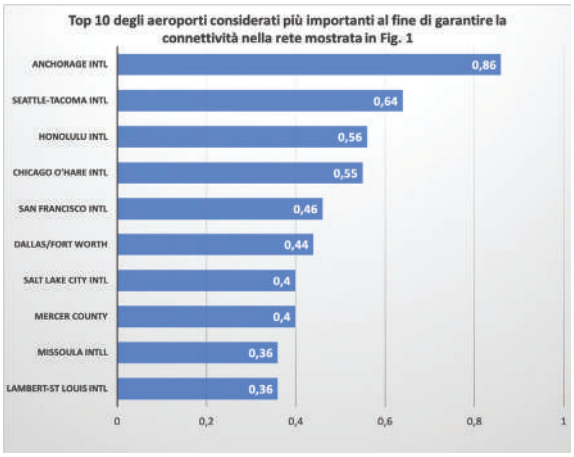


Figura 2 : Top 10 degli aeroporti considerati più importanti

La metodologia proposta è stata testata sulla rete mostrata in Figura 1, la quale rappresenta i voli aerei esistenti tra gli aeroporti degli stati uniti nel 1997. La rete è composta da 332 aeroporti e 4252 voli diretti. Ogni nodo rappresenta un aeroporto ed ogni collegamento l'esistenza di un volo diretto tra due aeroporti. I risultati riportati in Figura 2 evidenziano come nodi più critici della rete gli aeroporti di Anchorage, Seattle ed Honolulu, nonostante non siano gli aeroporti più connessi (cioè con più voli in partenza ed arrivo) ma risultano fondamentali per garantire la connessione tra tutti gli aeroporti del paese. L'andamento dei valori di criticità riportato in Figura 2 rappresenta gli aeroporti più appetibili ed interessanti per un gruppo di attaccanti con preferenze molto diverse tra loro e ne cattura gli aspetti in comune. Un aspetto molto interessante di tale studio è rappresentato dal fatto che un'allocazione di risorse per la protezione dell'infrastruttura, eseguita in maniera proporzionale agli indici appena individuali, incrementa sensibilmente la resilienza del sistema rendendo omogenea la distribuzione dei livelli di criticità tra i diversi nodi della rete.

Possiamo dunque concludere che tale studio intende spostare l'attenzione da quei nodi con funzione di hub centrali e fortemente connessi verso quei nodi che invece hanno la funzione di bridge e che spesso possono essere geograficamente periferici ma fondamentali al fine di garantire la connettività dell'infrastruttura.

Gli sviluppi futuri di tale studio sono mirati alla dimostrazione di come tale metrica possa essere alla base di piani di investimento per attuare politiche di protezione della rete, al fine di rendere l'infrastruttura più resiliente nei confronti di attacchi che mirano alla sospensione dei servizi che erogano. ■

Applicazioni sotto attacco: perché sono un target ideale

Il nuovo Application Protection Report di F5 Networks mostra quali siano le tecniche più utilizzate e gli obiettivi primari degli attacchi, anche nel nostro Paese

Autore: Maurizio Desiderio,
Country Manager di F5 Italia & Malta

Proteggere le applicazioni è sempre stato un compito fondamentale per la sicurezza e continuerà ad esserlo in futuro. Come l'ecosistema della barriera corallina, che brulica di una varietà enorme di vita, le applicazioni web sono "creature che vivono in colonie".

BIO

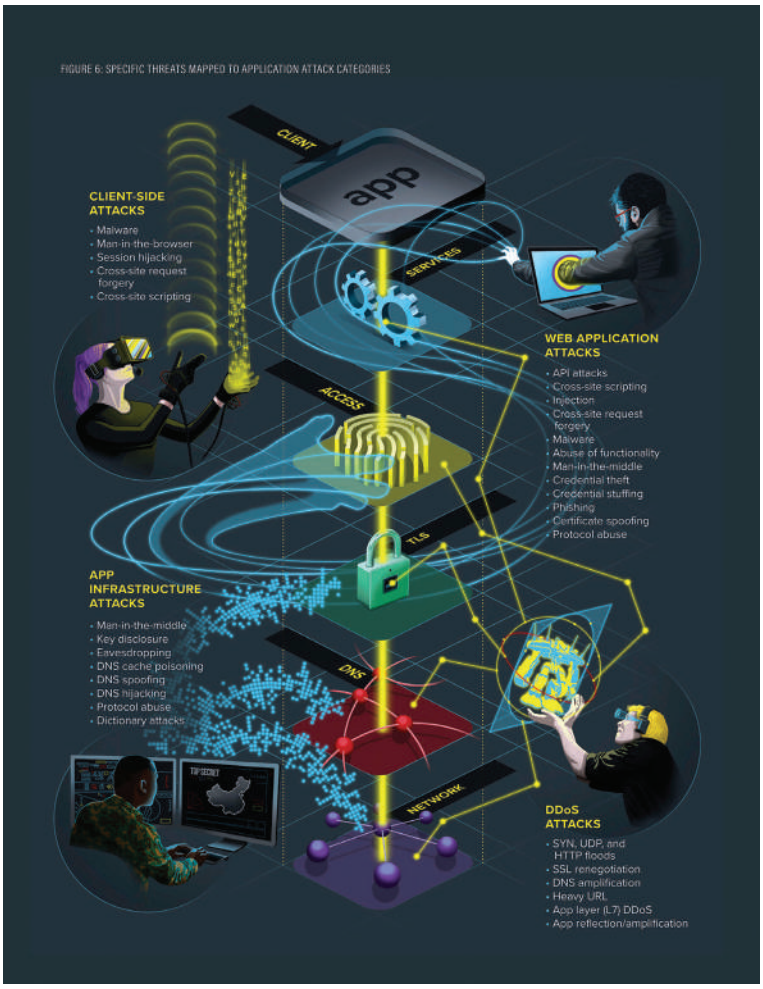
Maurizio Desiderio è Country Manager Italy & Malta di F5 Networks, con la responsabilità di guidare il business e definire la strategia di F5 Networks nella Region per espandere ulteriormente le attività dell'azienda, in particolare nelle aree della security, dell'application delivery e del deployment delle applicazioni cloud.
Da oltre 25 anni nel mercato IT, Maurizio ha maturato una grande esperienza nello sviluppo del business, nelle vendite e nella gestione del Canale e rivestito ruoli di crescente responsabilità all'interno di multinazionali in Italia e all'estero. Prima di approdare in F5 Networks, dal 2010 è stato *Sales Director Italia, Turchia e Medio Oriente* di Infoblox, occupandosi di guidare lo sviluppo, incrementare le vendite e la competitività e guidare la crescita della società.
Precedentemente, ha ricoperto il ruolo di *Direttore Commerciale Southern Europe and Middle East* per Imprivata, dal 2005 al 2010, e Sales *Director Italia e Grecia* per Novell dal 2003 al 2005.
Ha maturato inoltre esperienze significative nel Regno Unito dal 1989, occupandosi di vendite e consulenza di business in aziende come Silvestream, Staffware e Banctec.

Sono costituite da una moltitudine di componenti indipendenti, in esecuzione in ambienti separati con requisiti operativi e infrastrutture di supporto differenti (sia nel cloud che on premise), connesse tra loro tramite le reti. Esistono tutta una serie di livelli interattivi - servizi applicativi, accesso alle applicazioni, transport layer services (TLS), domain name services (DNS), e la rete stessa —e ognuno è un potenziale un bersaglio da attaccare.

Per ottenere un punto di vista oggettivo su come le applicazioni vengono attaccate, tramite i nostri F5 Labs, i laboratori di analisi e ricerca di F5 Networks, abbiamo esaminato i dati provenienti da una varietà di fonti, inclusi i set di dati interni, le vulnerabilità di WhiteHat Security, i dati di attacco di Loryka e un'indagine sulla sicurezza che abbiamo commissionato all'istituto di ricerca Ponemon dando vita all'edizione 2018 del Application Protection Report.

Secondo i dati raccolti su 301 violazioni segnalate nel corso del 2017 e nel primo trimestre del 2018 le violazioni nel 30% dei casi hanno riguardato le applicazioni Web. Ulteriori ricerche degli F5 Labs che hanno presso in esame 433 casi di violazioni di alto profilo avvenute nell'arco di 12 anni e in 26 paesi hanno rilevato che le applicazioni rappresentavano gli obiettivi iniziali dell'attacco in oltre la metà delle violazioni registrate (53%).

Quando le app vengono attaccate le ripercussioni possono essere gravi e molto diverse tra loro: tra quelle che preoccupano maggiormente gli intervistati troviamo il denial of service per l'impatto forte e immediato sull'organizzazione, indicato dall'81% degli intervistati e seguito dalle violazioni che compromettono informazioni riservate o sensibili (come la proprietà intellettuale o i segreti commerciali), con il 77% degli intervistati.



Quali sono le tecniche più usate e le vulnerabilità maggiormente sfruttate

Analizzando nel dettaglio le violazioni alle applicazioni abbiamo scoperto che la maggior parte ha riguardato **il furto dei dati delle carte di pagamento dei clienti tramite web injection** (70%), hacking di siti Web (26%) e hacking di database di app (4%).

Gli attacchi di web injection consentono a un utente malintenzionato di inserire comandi o nuovo codice direttamente in un'applicazione in esecuzione (processo noto anche come manomissione di un'app) per attivare uno schema dannoso. Negli ultimi dieci anni, **il 23% delle violazioni registrate ha coinvolto attacchi con SQL injection**, il tipo più subdolo di questa tipologia di attacco.

Le vulnerabilità alle injection (comprendendo le debolezze non ancora sfruttate) sono prevalenti. WhiteHat Security conferma questo dato, dichiarando che il 17% di tutte le vulnerabilità scoperte nel 2017 riguardava l'injection. Questo problema è talmente significativo che i difetti di injection sono considerati il primo rischio per le applicazioni nell'elenco OWASP Top 10 2017. Per questo motivo, è necessario dare priorità alla ricerca, all'applicazione di patch e al loro blocco.

L'analisi delle violazioni ha rilevato anche come il 13% di tutte le violazioni delle app Web nel 2017 e il primo trimestre 2018 sia legato all'accesso. In particolare, al furto delle credenziali tramite email (34,29%), all'errata

OWASP

OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

configurazione del controllo degli accessi (22,86%), agli attacchi brute force per crackare le password (5,71%), al credential stuffing per sottrarre le password (8,57%) e al furto tramite tecniche di social engineering (2,76%). Questo dato non stupisce se consideriamo, come evidenziano di dati di Ponemon Institute, che il 75% degli intervistati utilizzava solo nome utente e password per l'autenticazione dell'applicazione anche se si trattava di applicazioni Web critiche. In realtà, per qualsiasi tipologia di applicazione bisognerebbe prendere in considerazione soluzioni di autenticazione forti come l'identità federata o il multi-fattore.

Come proteggere le proprie applicazioni oggi

Alla luce dei risultati del report vorrei proporre 4 spunti di riflessione, consigli che potrebbero sembrare banali ma sono indispensabili come punto di partenza per una sicurezza applicativa concreta e valida.

Il primo riguarda la **"Comprensione dell'ambiente"**: sapere quali applicazioni si possiedono e a quali repository di dati hanno accesso non è semplice ma è indispensabile. La conoscenza è potere, è necessario sapere quali sono le app di cui la propria organizzazione ha bisogno e quelle da cui i propri clienti dipendono. Per quelle di propria proprietà si deve poter eseguire regolarmente la scansione e l'inventario, per le applicazioni esterne da cui dipendono gli utenti, invece, ci può scegliere di affidarsi un cloud access security broker (CASB) per tenerle sotto controllo e monitorarne l'utilizzo. Proteggere le app interne, comporta anche riuscire ad instaurare una buona comunicazione con i propri sviluppatori così da avere sotto controllo le applicazioni, i piani futuri che le riguardano e gli ambienti di sviluppo.

Al secondo posto, ma a parimerito per importanza, metterei la necessità di **ridurre la superficie di attacco** perché qualsiasi aspetto di un servizio applicativo visibile su Internet, direttamente o indirettamente, sarà analizzato dagli hacker alla ricerca di possibili vulnerabilità da sfruttare. Oggi abbiamo a che fare con superfici sempre più ampie, a causa dei livelli multipli di un'app e l'utilizzo sempre crescente delle API (Application Programming Interface) per la condivisione dei dati con terze parti. Tutto

quello che viene esposto tramite Internet deve essere controllato dal punto di vista dell'accesso, deve essere aggiornato e rinforzato in vista di possibili attacchi. Un buon firewall per applicazioni web (WAF), che per altro è il primo strumento indicato dagli intervistati nel nostro Application Protection Report, può fare guadagnare il tempo necessario per fare tutto questo, eseguendo ad esempio "patch virtuali" analizzando il traffico delle applicazioni e bloccando gli attacchi di exploit noti.

Il terzo passaggio è quello di **assegnare la priorità alle difese in base al rischio**. Una volta stabilito quali applicazioni sono importanti e aver ridotto al minimo la superficie di attacco, si deve identificare le applicazioni che richiedono risorse aggiuntive. Anche un'analisi del rischio non perfetta è comunque migliore di ipotesi casuali o di un processo decisionale distorto. I dati hanno il potere di guidare la strategia di rischio e aiutarci a capire cosa potrebbe interessare chi ci attaccherà.

La scelta della tecnologia, con **l'adozione di strumenti di difesa flessibili e integrati**, resta, infine, fondamentale per il rilevamento e ripristino da minacce esistenti ed emergenti. La protezione deve estendersi a tutti i livelli da cui dipende un'applicazione. A ogni applicazione deve essere fornito il proprio perimetro di protezione, che la abbracci integralmente con la protezione dal DDoS e la definizione di policy private di sicurezza applicativa.

In questo contesto la formazione deve essere continua perché oltre ad essere coerenti, le soluzioni di sicurezza dovrebbero essere ben comprese da chi si occupa di sicurezza in aziende; spesso purtroppo le violazioni si verificano nonostante vi siano delle soluzioni implementate, semplicemente a causa di un malinteso o di una errata configurazione di un prodotto. I dati della ricerca confermano che la mancanza di personale qualificato o esperto è la principale barriera principale per la sicurezza applicativa, in uno scenario che purtroppo è non può che peggiorare se consideriamo che già oggi un'organizzazione utilizza in media 765 diverse applicazioni Web e l'outsourcing della sicurezza delle applicazioni è destinato a crescere, sia che si tratti di funzioni di sicurezza come anti-DDoS o monitoraggio della sicurezza delle applicazioni Web oppure del passaggio a piattaforme hosted che forniscono servizi di sicurezza come parte della loro offerta.

In sintesi, credo che dalle nostre ricerche emerga la sempre maggiore urgenza di proteggere tutte le applicazioni, come veicolo fondamentale di accesso al patrimonio delle aziende.

Proteggere le applicazioni ovunque si trovino significa, infatti, in sostanza, protegge la propria identità e riuscire ad adattarsi rapidamente a un ambiente digitale in continua trasformazione. ■

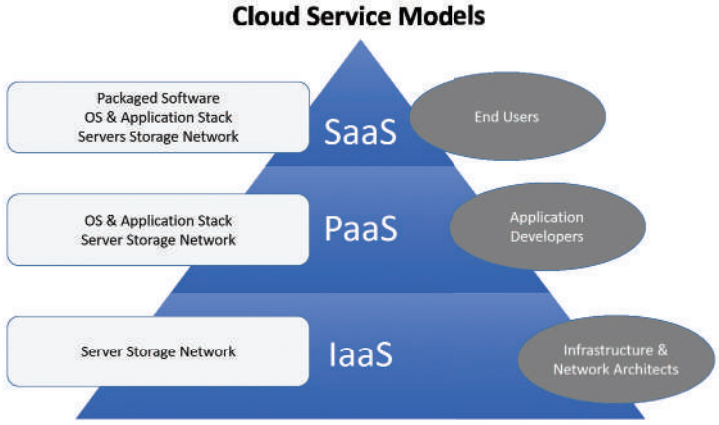
Una cosa divertente da raccontare mentre si transita al cloud

Autore: **Greg Hanson,**
Informatica Vice President Sales Specialists and CTO

Il cloud computing prometteva di semplificare enormemente il modo in cui le organizzazioni gestivano e accedevano a applicazioni, dati e infrastrutture quando emersero per la prima volta due decenni fa. Cloud era il biglietto d'oro non solo per la semplicità, ma per ridurre i costi e aumentare l'agilità.

Infatti, secondo uno studio di KPMG, la motivazione numero uno nel 2017 per passare al cloud è stato l'aumento di agilità. L›ironia, tuttavia, è che nel percorso verso una maggiore agilità, siamo inciampati in un mondo ibrido composto da più soluzioni cloud e on-premise.

La promessa del cloud ha incontrato la realtà di una maggiore complessità. E la nuova realtà ha provocato un›enorme sfida nella gestione dei dati, con le informazioni che vivono su più cloud IaaS, PaaS e SaaS mentre le organizzazioni «scelgono il cloud giusto per il lavoro.» AWS può essere la scelta in un caso, Microsoft Azure in un altro, Google Cloud nel terzo e Salesforce nel quarto e così via, con i dati sparsi su tutti loro.



Uno degli obiettivi di una strategia multi-cloud è quello di consentire un approccio best-breed al cloud ed evitare il lock-in su un unico fornitore di cloud. Ma introduce anche la frammentazione dei dati e delle competenze, che a sua volta riduce l›agilità, rendendo difficile il raggiungimento delle trasformazioni digitali guidate dai dati che le aziende ricercano per guidare il loro vantaggio competitivo sul mercato.

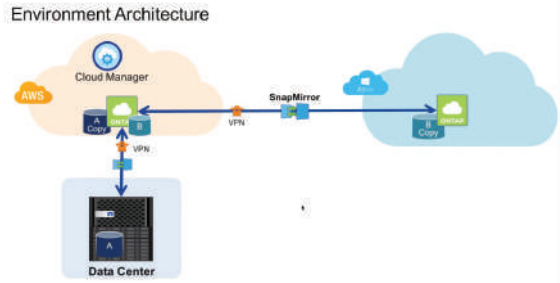
Cloud pubblici e privati e cloud di analisi come Google BigQuery, Amazon Redshift e Snowflake Elastic Data Warehouse, aggiungono complessità e sfide alla gestione dei dati. E la complessità multi-cloud aumenterà mentre le organizzazioni continuano ad adottare rapidamente i servizi cloud.

Ad esempio, Gartner, Inc., prevede che i ricavi del servizio cloud pubblico in tutto il mondo raggiungeranno $ 302,5 miliardi entro il 2021, quasi raddoppiando rispetto al totale del 2017. Nel frattempo, nove delle 10 aziende avranno almeno alcune applicazioni o un'infrastruttura nel cloud entro il 2019, secondo il Global Cloud Computing Study 2018 IDG.

Tuttavia, i sistemi on-premises mission-critical rimarranno in essere per il prossimo futuro e dovranno interagire con quelli nel cloud per scambiare dati e supportare l›automazione dei processi. Le organizzazioni cloud-first possono avere la testa nel cloud, ma almeno uno dei loro piedi può rimanere piantato in un ambiente locale.

BIO

Greg è il CTO EMEA e America Latina di Informatica. Come CTO agisce da customer champion mantenendo i rapporti tra i clienti e Informatica. Ciò gli consente di sviluppare una profonda comprensione dei clienti, delle loro sfide, delle necessità di governance e compliance, così come del mercato in cui operano e delle modalità con cui sfruttare i dati per avere successo ed essere competitivi. Greg è anche responsabile per le vendite in EMEA e America Latina di tutte le linee di prodotti di Informatica, inclusi Master Data Management, Data Quality, Data Governance, Sicurezza dei dati e Integration Platform as a Service (Cloud/Hybrid integration).
Greg ha più di 20 anni di esperienza nella creazione di team di successo nell'ambito del data management. Prima di entrare in Informatica dove ha creato un team di consulenza pre-vendita e di settore per l'EMEA e l'America Latina, si è occupato di project management, delivery di soluzioni di data warehouse e di soluzioni analitiche.



Gestione dei dati in ambienti ibridi multi-cloud

Con l'accumulo di dati su più cloud pubblici e privati, così come i sistemi interni, le organizzazioni stanno facendo domande difficili come:

- Come possiamo garantire l'interoperabilità tra diversi paesaggi IT?
- Come possiamo offrire una visione dei dati pulita, coerente, completa e affidabile in tutte le applicazioni?
- Come rileviamo e proteggiamo efficacemente le informazioni sensibili?
- Come possiamo rendere i dati unificati, accessibili e utilizzabili quando esistono in un ambiente ibrido multi-cloud?

I rischi per le aziende e l'IT aumentano quando i dati si moltiplicano in ambienti ibridi multi-cloud. Senza un approccio olistico e ben governato, le organizzazioni devono affrontare complicazioni in casi d'uso come l'analisi aziendale e la gestione dell'esperienza del cliente (CX).

Oggi, ogni organizzazione è alla ricerca di CX, in quanto può fornire risultati notevoli in termini di coinvolgimento, fatturato e fedeltà dei clienti. Tuttavia, le sole applicazioni CRM possono darti un falso senso di sicurezza, in quanto promettono di offrire un'ottima CX, ma spesso mancano di una visione pulita, coerente, completa e affidabile di un cliente, che è amplificata in un ambiente multi-cloud.

Per fare bene CX, è necessaria una perfetta interoperabilità, governance dei dati e scambio di dati, soprattutto se un'applicazione di marketing vive in un cloud e un sistema CRM in un altro; mentre uno strumento BI, il data warehouse e l'applicazione ERP rimangono locali.

Con questo grado di frammentazione, diventa più difficile raggiungere la visione a 360 gradi dei clienti che le vendite e il marketing devono comprendere i clienti, anticipare le loro esigenze e interagire con le interazioni pertinenti e tempestive sul canale giusto. Tecniche di integrazione tradizionali e limitate con API, codifica manuale e strumenti centrati sull'applicazione non sono adatte per risolvere i problemi di gestione dei dati in paesaggi ibridi multi-cloud.

"Dati puliti, affidabili e sicuri" al centro dei processi aziendali

Le organizzazioni leader in tutti i settori stanno adottando un approccio di prossima generazione. Un esempio è Genomic Health, un fornitore di test diagnostici basato sulla genomica basato sulla Silicon Valley che aiuta a ottimizzare la cura del cancro. Genomic Health utilizza la gestione intelligente dei dati ibridi su diversi sistemi che includono Salesforce basato su cloud e applicazioni locali che ospitano grandi volumi di dati sensibili relativi a pazienti, medici, clinici e altre informazioni.

"La possibilità di connettere le applicazioni indipendentemente dal fatto che siano nel cloud o in locale e farlo in tempo quasi reale per ottenere informazioni utili per l'utente business giusto, è la cosa a cui tengo ogni giorno", David Green , senior director of IT and Informatics presso Genomic Health.

"Avere dati puliti, affidabili e sicuri al centro di ciò che sta guidando tutti i nostri sistemi e processi aziendali è incredibilmente importante", ha aggiunto Green. "Senza la possibilità di riunire queste diverse fonti di dati, combinarle in modi unici e convincenti per raccontare una storia particolare o affrontare un problema aziendale, resteremo bloccati".

La gestione intelligente dei dati ibridi è particolarmente importante per le società globali in crescita come cloud, come Genomic Health, i cui test di espressione genica hanno contribuito a guidare le decisioni di trattamento per oltre 900.000 pazienti oncologici in tutto il mondo. Supporta inoltre le iniziative di Genomic Health per aggiungere nuove linee di business, comprendere meglio e coinvolgere i medici ed espandersi a livello internazionale, il tutto mantenendo la conformità normativa.

In un mondo cloud-first, la piattaforma di integrazione basata sul cloud come servizio (iPaaS) è una soluzione naturale per affrontare le sfide di integrazione in ambienti ibridi multi-cloud.

Ma iPaaS deve andare oltre l'applicazione di base e l'integrazione dei dati. Dovrebbe inoltre affrontare problemi di qualità, coerenza e sicurezza critici con tutte le funzionalità della gestione dei dati cloud, tra cui:

- **Qualità dei dati.** Garantisce la precisione dei dati, elimina i duplicati e corregge continuamente i problemi per garantire che l'azienda abbia informazioni attendibili e contestualizzate.
- **Gestione dei dati master.** Offre una visione a 360 gradi dei dati sulle entità aziendali (ad es. Cliente, fornitore, partner) su tutte le fonti di dati, inclusi i dati di transazione e di interazione.
- **Privacy e protezione dei dati.** Aiuta a identificare rapidamente i dati sensibili, a rimediare ai problemi con le raccomandazioni guidate dall'IA e a rispettare le normative e le politiche di sicurezza dei dati.

Senza queste funzionalità, alle organizzazioni vengono lasciate carenze di dati che possono sovvertire gli obiettivi aziendali. E sono mal equipaggiati per affrontare i cambiamenti continui mentre tecnologie come IoT, AI, Blockchain, criptovaluta e altre maturano.

L'opportunità qui è di introdurre la gestione dei dati che è costruita su una base di intelligenza artificiale guidata da metadati, attraverso il tuo ambiente ibrido multi-cloud per combattere la complessità e garantire che i dati siano completi, accurati e aggiornati.

Ciò si ripaga immediatamente in migliori relazioni con i clienti, decisionale informato ed efficienza operativa. Inoltre, resiste a future esigenze di gestione dei dati con l'adattabilità per la prossima ondata di interruzioni IT.

Alla fine, il biglietto d'oro potrebbe non essere semplice come scegliere il cloud, ma con una gestione intelligente dei dati ibrida si può spianare la strada verso il successo. ■

Sviluppo sicuro del codice... 4 semplici domande a 3 strati di una cipolla

Autore: Massimiliano Brolli

Sempre più spesso, in grandi organizzazioni, si parla di Sviluppo Sicuro del Codice (di seguito SSC) ovvero strumenti automatici a supporto dei programmatori che consentono di analizzare il software prodotto alla ricerca di vulnerabilità (tipicamente Owasp TOP10 o SANS25) da sanare prima del rilascio per rendere un software robusto a prova di intrusione.

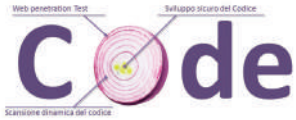
Ma questo approccio premia davvero?

Esistono differenti modi di effettuare test di sicurezza applicativi, tutti basati nel rilevare errori di programmazione e di implementazione delle logiche applicative, ma la pratica dello sviluppo sicuro risulta sempre lo strato più delicato ed "insicuro" per produrre applicazioni "rock-solid".

BIO

Attualmente responsabile delle funzione di monitoraggio dei piani di sicurezza e delle attività di risk Assessment sui sistemi TIM e società partecipate, ha rivestito diversi incarichi manageriali in Telecom Italia e TIIT (Telecom Italia Information Tecnology) spaziando da attività di governance e Audit di sicurezza ad attività di gestione applicativa di piattaforme centralizzate con un passato nello sviluppo del software in società come IBM, 3inet, Praxi e Bnl oltre a numerose attività di docenza svolte su ambiti come uml, object oriented e differenti framework e linguaggi di programmazione.

Occupandomi di verifiche di sicurezza, molto spesso mi sono imbattuto nel rilevare negli assessment impatti derivanti l'abuso di vulnerabilità non sanate nello SSC e molto spesso di tali vulnerabilità non vi era traccia nei report prodotti dagli strumenti di scansione statica. Ma prima di darvi una visione di dettaglio delle mie considerazioni dobbiamo porci una domanda: "che cosa è una scansione statica del codice?" Se per voi la risposta è *"un tool che consente di identificare tutte le problematiche di sicurezza applicative che possono mettere a rischio la nostra applicazione"*, siete completamente fuori strada.



Infatti gli strumenti di scansione statica (ma come vedremo successivamente anche dinamica, tralasciando quanto dichiarato dai fornitori dei tool) consentono di rilevare, con buona confidenza, vulnerabilità tipiche di depurazione dell'input quali XSS ed *Injection.

La tabella in calce (Fonte Owasp con qualche arricchimento) pone attenzione su questo problema, ma lascio a voi le dovute considerazioni.

ID Owasp	Vulnerabilità	Sfruttamento	Diffusione	Individuazione con strumenti automatici	Impatto
A1	Injection	Facile	Comune	Medio	Severo
A2	Broken Authentication	Facile	Comune	Difficile	Severo
A3	Sensitive Data Exposure	Medio	Diffuso	Medio	Severo
A4	XML External Entities (XXE)	Medio	Comune	Facile	Severo
A5	Broken Access Control	Medio	Comune	Difficile	Severo
A6	Security Misconfiguration	Facile	Diffuso	Facile	Medio
A7	Cross-Site Scripting (XSS)	Facile	Diffuso	Facile	Medio
A8	Insecure Deserialization	Difficile	Comune	Medio	Severo
A9	Using Components with Known Vulnerabilities	Medio	Diffuso	Medio	Medio
A10	Insufficent Logging & Monitoring	Medio	Diffuso	Difficile	Medio

Il problema principale, analizzando nel dettaglio le TOP10 Owasp, è che esistono vulnerabilità con impatti molto severi che non vengono rilevate dagli strumenti automatici e tali vulnerabilità sono comportamenti "applicativi" o errori (spesso orrori) di progettazione che non possono essere rilevati dagli strumenti di oggi.

Ad esempio *Broken Authentication* e *Broken Access Control* sono vettori di attacco formidabili che conducono ad impatti molto severi senza pensare ad una SQL Injection difficile da rilevare, quindi la scansione statica porta con sè dei limiti in quanto:

- Non mette al riparo dalla presenza di errori nella logica applicativa proprio gli ambiti di sfruttamento più critico come ad esempio carenze nello sviluppo della profilazione e nel principio del need to know, ovvero consentire l'accesso ai contenuti sui quali si è autorizzati.
- Introduce molti Falsi positivi (oltre il 50% delle rilevazioni sono tali) e ancora più rischiosi e fuori controllo sono i Falsi negativi, ovvero vulnerabilità reali non identificate spesso SQL injection.
- La bontà della scansione risulta dipendente dall'istruzione degli scanner e dell'ambiente di scansione (ad esempio dipendenze tra librerie, dipendenze tra moduli applicativi, framework di terze parti utilizzati e warning di scansione non gestiti).

Ma il "cattivo" non lavora in sviluppo ma in produzione e magari dalla Cina o dalla Russia, quindi potrebbe venire lecita la seconda domanda: "...ma se sposto il controllo in produzione utilizzando scanner dinamici potrei avere maggiori margini di confidenza?" La risposta è la stessa di quando si confronta un uomo e una macchina. Ma al netto della risposta la scansione dinamica (ad esempio gli strumenti di web scanning) sono utili come tutti i Vulnerability Assessment perché spostano il controllo più vicino all'attività illecita ma anche in questo caso sono presenti una serie di limitazioni da considerare:

- Gli scanner web non mettono al riparo dalla presenza di errori applicativi di sviluppo del software (come visto in precedenza nelle scansioni statiche) anche se hanno un ventaglio maggiore di copertura proprio perché eseguite in campo.
- Uno Scanner dinamico è molto intrusivo, pertanto è buona pratica farlo in collaudo per salvaguardare l'esercizio, ma facendolo in collaudo si introducono possibili elementi di debolezza come ambienti disomogenei, versioni software differenti, patch differenti, ambienti di collaudi non disponibili, ecc...
- L'intrusività delle policy è direttamente proporzionale alle vulnerabilità rilevate. E' importante avere esperienza in tal senso per ottenere il giusto compromesso.
- A differenza delle tecnologie e dalle policy definite può introdurre Falsi positivi e i più rischiosi Falsi negativi.

Quindi siamo arrivati alla terza domanda: "... ma allora, forse è meglio lasciare perdere tutto per avviare dei Penetration Test Applicativi?". Potrebbe essere una soluzione, ma anche in questo caso ci sono dei punti di attenzione da prendere in considerazione in quanto:

- Un PT web si fa direttamente in esercizio e dà un buon grado di confidenza del rischio presente nell'applicazione e risulta poco invasivo in quanto svolto da un tecnico specializzato e l'efficacia è direttamente proporzionale agli skill del personale specializzato.
- In applicazioni complesse non può essere praticabile su tutte le "foglie" dell'applicazione per i limiti temporali di gestione di un controllo (un PT non è un Ethical-APT a livello temporale).
- Consente di identificare gli "Impatti reali" ed è efficace nel rilevare carenze dove risulta impossibile l'identificazione con scansioni statiche/dinamiche.
- Fornisce un quadro completo (anche abbinandolo a una scansione web) del reale grado di rischio dell'applicazione.
- Ha dei costi superiori alle consuete attività automatizzate.

Quindi ci posizioniamo sulla quarta domanda …" e allora? ... qual è la soluzione migliore da adottare?", la risposta come al solito è "dipende" in quanto:

1. Lo Sviluppo Sicuro del Codice è demandato alle fabbriche, serve a "rastrellare" tramite scansione statica le falle di sicurezza più semplici e deve essere fatto. Inoltre l'utilizzo di questi scanner (inteso come tool di sviluppo allo stesso livello di un Eclipse o un VisualStudio) crea valore indiretto introducendo "Consapevolezza" nei Team di sviluppo, molti di questi ancora oggi con grosse lacune in termini di sviluppo sicuro del software.
2. La scansione dinamica (come tutti i vulnerability assessment) è il "setaccio a grana grossa", è utile, porta benefici e vulnerabilità spesso reali ma occorre prestare molta attenzione sui rischi in produzione, sull'invasività dei prodotti di scansione scelti, sulle policy utilizzate rispetto a quanto visto in precedenza.
3. Il Penetration test Applicativo è la soluzione ideale per avere una buona confidenza sui rischi derivanti un abuso della nostra applicazione in quanto riesce a coprire tutte le TOP10 Owasp, ma un PT su una applicazione complessa potrebbe avere costi proibitivi oltre ad essere a livello di tempistiche poco sostenibile.

Concludendo, tutte e tre le tecniche (scansione statica, dinamica e PT Applicativo) sono tecniche che forniscono raramente risultati sovrapponibili, sarà la nostra esperienza a metterle a fattor comune per individuare il livello di sovrapposizione e i delta delle vulnerabilità rilevate.

Il rischio Zero non esiste (pensiamo all'incidente del 28/09/2019 di Facebook denominato "view as" che ha portato al reset di 100mln di token) ma esiste il rischio "tollerabile". Tutte e tre le tecniche dovranno quindi essere misurate per comprendere dove una sia migliore dell'altra, dove dovranno essere scelte tecniche miste, anche in funzione dell'appetibilità dei dati contenuti all'interno delle nostre applicazioni. Su applicazioni con dati critici, personalmente utilizzo tutte e tre le tecniche mentre su applicazioni con dati non critici, anche la sola scansione statica può risultare una scelta sensata.

E' chiaro che chi sviluppa software non può limitarsi all'utilizzo di uno strumento di scansione ma deve essere guidato dall'esperienza e dall'applicazione delle migliori best practices conosciute in termini di sviluppo sicuro del codice. Per chi usa e abusa di forniture esterne, risulta di focale importanza l'aspetto contrattuale articolato su deliverable differenti a seconda della criticità dei sistemi.

Effettuando un paragone, mi viene da pensare ai guasti difficili da identificare in una macchina di oggi e i meccanici che collegano la centralina al computer e fanno solo quello che lo scanner dice nelle attività di riparazione. Altri meccanici invece che conoscono a fondo tutte le componenti del veicolo comprendono che quanto fornito dallo scanner potrebbe essere una indicazione di un difetto presente in un'altra parte non chiaramente identificata, identificabile univocamente dalla loro esperienza. ■

Dalle Università

L'Università di Genova individua un attacco di phishing per rubare le credenziali salvate su smartphone android

Un gruppo di ricercatori dell'Università di Genova: il prof. Alessio Merlo, il dottorando Simone Aonzo e lo studente Giulio Tavella, in collaborazione con Yanick Fratantonio di Eurecom, ha individuato un pericoloso attacco di phishing su Android che permette di rubare le credenziali dell'utente per l'accesso a servizi critici (home banking, trading, pagamento elettronico, social network, servizi istituzionali, ...) salvate sui *password manager*.

Il team di ricercatori ha evidenziato che, seppur esista una soluzione tecnica, la risoluzione del problema non può essere immediata e non dipende esclusivamente dagli sviluppatori di password manager o del sistema operativo Android, ma richiede uno sforzo globale da parte delle comunità Web e Android.

Il team di ricercatori ha segnalato il problema sia ai principali sviluppatori di password manager mondiali che al Security Team di Android con cui ha collaborato attivamente per mitigare il problema. ■

L'Università Campus Bio-Medico di Roma vince il premio dedicato ai più innovativi progetti di ricerca internazionale sulla sicurezza delle infrastrutture critiche portati avanti da giovani ricercatori.

Il gruppo italiano formato da Luca Faramondi, Gabriele Oliva, Stefano Panzieri e Roberto Setola dell'Università Campus Bio-medico di Roma si è aggiudicato il secondo posto dello Young CRITIS award, il premio dedicato ai migliori progetti di ricerca internazionale di giovani ricercatori.

Nella ricerca "Discovering vulnerabilities in heterogeneous interconnected systems"(Scoperta della vulnerabilità in sistemi interconnessi eterogenei), vincitrice del premio, i ricercatori hanno valutato la vulnerabilità nelle reti di infrastrutture critiche soprattutto in caso di un attacco intenzionale al fine di poter implementare idonee strategie di protezione e garantire una maggiore resilienza.

L'individuazione delle criticità è il primo passo per una corretta allocazione dei fondi, la ricerca presentata vuole proporre un nuovo modo di investire nella protezione delle infrastrutture critiche ponendo l'attenzione sul mantenimento della connettività, requisito funzionale necessario alla fruizione dei servizi associati a tali infrastrutture. ■

L'Università della Calabria uno dei nodi del CyberChallege 2019

Riparte anche per il 2019 la CyberChallenge.IT, il primo programma italiano di formazione per giovani talenti in cyber security. La sfida, che interesserà varie sedi universitarie sparse sul territorio nazionale, vedrà quest'anno protagonista anche l'Università della Calabria.

L'obiettivo del programma è di formare nuove generazioni di innovatori nel campo della cyber security. I vincitori della scorsa edizione sono potuti entrare nella nazionale hacker italiana e rappresentare l'Italia al contest europeo di Londra. ■

Ancora aperte le iscrizioni al Master of Science in Cybersecurity in lingua inglese presso l'Università di Roma «La Sapienza»

Il Master of Science in Cybersecurity è la prima Laurea Magistrale in Italia a mettersi in linea con le nuove opportunità di specializzazione in materia di sicurezza informatica. L'intento è offrire una comprensione approfondita, completa e multi-disciplinare degli aspetti tecnologici, legali e manageriali che un esperto di Cybersecurity deve padroneggiare per rivestire un ruolo professionale di alto profilo. Gli studenti diventano così professionisti capaci di comprendere a livello tecnico le sfide di oggi e capaci di restare in costante aggiornamento su un terreno che propone sempre nuove frontiere.

La Sapienza ha creato questo corso in puntuale risposta anche alle stringenti esigenze dell'Industria 4.0 in una situazione economica nazionale e internazionale che richiede una nuova task-force di esperti in Cybersecurity.

Si selezionano studenti italiani, europei e internazionali al fine di offrire loro la possibilità di partecipare, in una forma ancora più strutturata e caratterizzante, al grande progetto formativo che la Sapienza ha portato avanti negli ultimi quindici anni attraverso i vari master universitari in sicurezza informatica. Proprio per garantire la massima apertura e vicinanza agli studenti, il corso è presente sui social alla pagina Facebook (www.facebook.com/cybersecSapienza/) e sul profilo LinkedIn (www.linkedin.com/in/master-of-science-cybersecurity-sapienza), nonché sul sito ufficiale https://cybersecurity.uniroma1.it/. ■

Aperte le iscrizioni per l'edizione del master del Campus Bio-Medico in Homeland Security 2019 con possibilità di borse di studio

Il Master universitario di II livello in "Homeland Security – Sistemi, metodi e strumenti per la security e il crisis management" è un corso di formazione avanzata che mira a formare tecnici e professionisti in grado di elaborare un processo di analisi delle esigenze di sicurezza, identificare contromisure da adottare, progettare e sviluppare soluzioni integrate per ciò che riguarda l'attuazione, la gestione e l'esercizio di procedure e sistemi di sicurezza.

L'Università Campus Bio-Medico di Roma mette a disposizione fino a un massimo di 2 borse di studio a copertura totale e 6 a copertura parziale della quota di iscrizione e partecipa inoltre a bandi Inps e di altri enti per l'assegnazione di borse di studio a favore di partecipanti afferenti a specifiche categorie. È prevista inoltre l'iscrizione gratuita per il partecipante che, in fase di selezione, sarà identificato come manager didattico. https://www.unicampus.it/risorse-e-uffici/master-ecm-formazione-permanente/master-e-perfezionamento/master-e-perfezionamento/70251-master-di-ii-livello-in-homeland-security-edizione-11 ■

Realizzata per essere esposta nel 2013 all'ITU (l'Unione Internazionale delle Telecomunicazioni), premiata dall'ITU e quindi tradotta ed esposta consecutivamente in 28 città di Romania, Polonia e Svizzera, la mostra è stata tradotta in italiano per le Poste Italiane, col patrocinio della Polizia Nazionale. E stata presentata in anteprima nel 2016 presso la "MakerFaire – European Edition" di Roma (dove ha superato i 130.000 visitatori). In 30 pannelli, l'esposizione illustra l'evoluzione delle tecniche di comunicazione e di manipolazione delle informazioni dai tempi più antichi ai social media usati oggi da tutti. Consente senza essere moralizzatrice di educare giovani ed adulti ad una fruizione consapevole e protetta di Internet.
La mostra è integralmente visitabile sul sito del Distretto di Cyber Security delle Poste Italiane, dove l'esposizione reale è allestita in modo permanente:
https://www.distrettocybersecurity.it/mostra-2/

Una pubblicazione

web for business
swiss webacademy

A cura del

Global Cyber Security Center

Redazione:
Laurent Chrzanovski e Romulus Maier (†) (tutte le edizioni)
Per l'edizione del GCSEC:
Nicola Sotira, Elena Agresti

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Indirizzi:
Viale Europa 175 - 00144 Roma, Italia
Tel: 06 59582272
info@gcsec.org
Şcoala de Înot nr.18, 550005,
Sibiu, Romania

www.gcsec.org
www.cybersecuritytrends.ro
www.swissacademy.eu

CERT STAR PROGRAM

COS'E'

CERT STAR è volto ad alimentare le competenze, promuovere la cooperazione e la condivisione di esperienze.

Nel corso degli incontri saranno svolte analisi tecnico-operative delle principali tematiche "core" di security: threat hunting, incident prevention e response, intelligence, analisi forense, comprensive di esercitazioni pratiche con tool tecnologici.

Gli incontri sono su invito, rivolti ad analisti e operatori dei CERT e dei SOC di grandi aziende, Pubblica Amministrazione e Forze dell'Ordine.

CALENDARIO

Sei incontri a Roma, dedicati a:

- ⇒ 26 febbraio – Cyber Range
- ⇒ 04 aprile – Dark web intelligence
- ⇒ 11 giugno – Digital forensics
- ⇒ 12 settembre – Inserire, classificare e condividere IoC con altri enti
- ⇒ 07 novembre – End point security
- ⇒ 03 dicembre – Incontro executive

SPONSORSHIP

Il pacchetto di sponsorizzazione comprende:

- ⇒ Logo dello sponsor sui materiali di marketing
- ⇒ Incontro con speech iniziale e sessione formativa dello sponsor
- ⇒ Presenza di personale dello sponsor agli accrediti
- ⇒ Distribuzione dei materiali di marketing dello sponsor
- ⇒ Video intervista su www.cybertrends.it
- ⇒ Articolo sulla rivista Cybersecurity Trends

LOCATION

- ⇒ Hotel Radisson Blue 4* – Via Filippo Turati, 171Roma
- ⇒ Poste Italiane, viale Europa 175 Roma

forum Software Industriale

MILANO
06_02_2019
Museo Nazionale Scienza e Tecnologia Leonardo Da Vinci
Sala Cavallerizze, Via Olona 6 bis

L'evoluzione delle tecnologie software nell'industria 4.0

Evento a partecipazione gratuita con riconoscimento crediti formativi

I TEMI DEL FORUM

- SMART MANUFACTURING
- VIRTUAL MANUFACTURING AND AUGMENTED REALITY
- INTELLIGENT AND CONNECTED PRODUCT
- INDUSTRIAL CYBER SECURITY

Aggiornamenti e registrazione www.forumsoftwareindustriale.it

ANIE AUTOMAZIONE

messe frankfurt