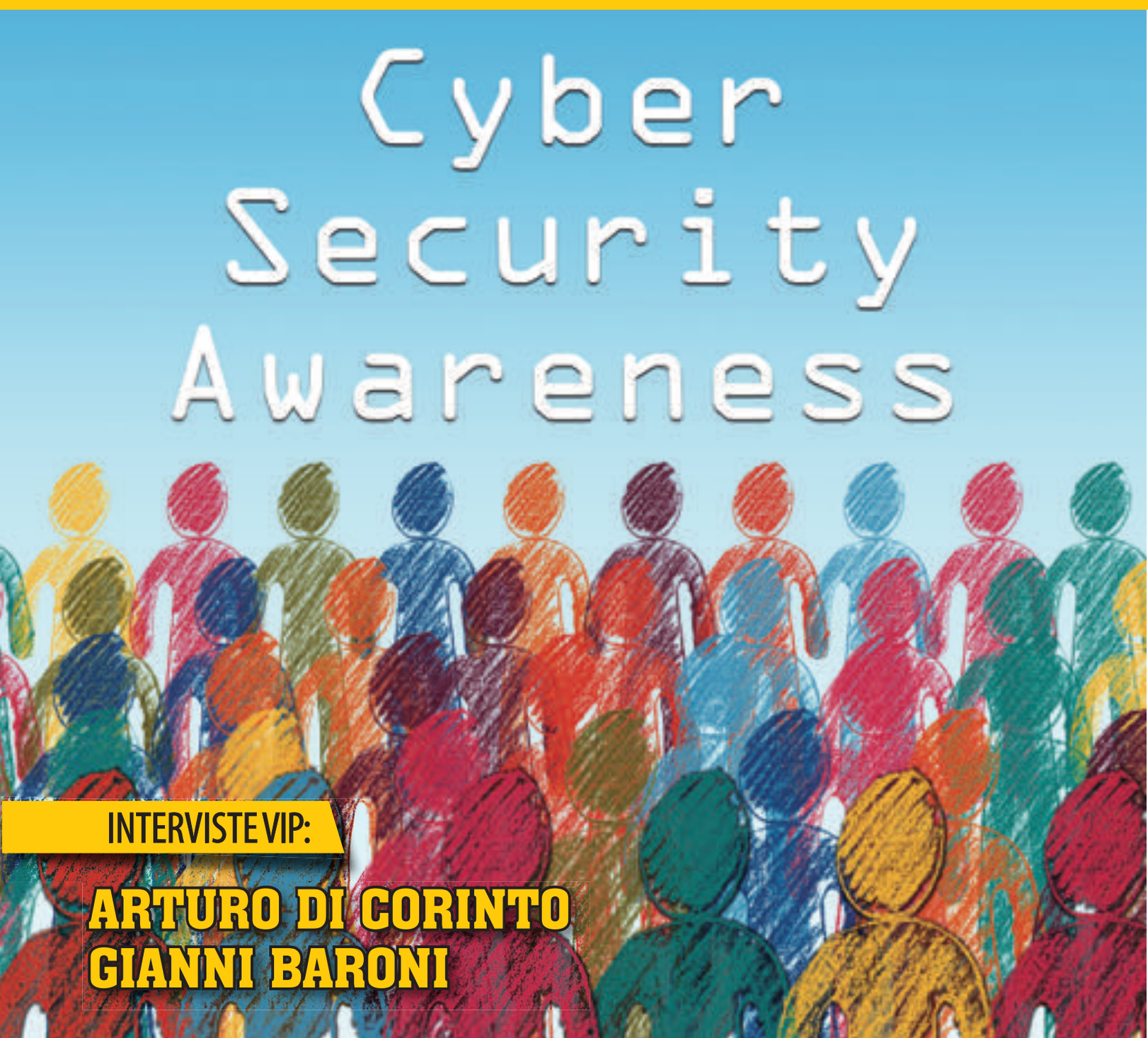
Cybersecurity Trends

Edizione italiana, N. 4 / 2019



INTERVISTE VIP:

ARTURO DI CORINTO
GIANNI BARONI

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Folder centrale: AWARENESS

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

2	**Editoriale: Vivere OnLife.** Autore: Nicola Sotira
3	**Educare e sensibilizzare, obiettivi chiave della Fondazione GCSEC.** Autore: Elena Mena Agresti
6	**Intervista VIP: Cinquant'anni di Internet a colloquio con Arturo di Corinto.** Autore: Massimiliano Cannata
10	**OcchioAlClic!** **La campagna di awareness 2019 del CERTFin.**
12	**Intervista VIP Gabriele Faggioli, presidente del Clusit.** Autore: Massimiliano Cannata
15	**Tecnologia e utenti uniti nel contrasto al phishing.** Autore: Roberto Cantarini
18	**Intervista VIP a Gianni Baroni, A.D. Daman Group e Cyber Guru S.R.L.** Autore: Massimiliano Cannata
21	**L'importanza dell'Awareness per la Sicurezza Informatica: il progetto CyberReadiness.IT** Autori: Marco Angelini, Claudio Ciccotelli
24	**Sicurezza e privacy: una inconsapevolezza diffusa.** Autore: Giancarlo Butti
28	**Awareness 2020 in Europa. Perché è già troppo tardi, tranne che per i nati della classe 2010.** Autore: Laurent Chrzanovski
35	**Convergenza e complementarità tra perimetro di sicurezza nazionale cibernetica edirettiva NIS.** Autore: Gianluca Bocci
38	**Intervista VIP a Rick McElroy, Responsabile Cyber Strategy, CARBON BLACK.** Autore: Elena Mena Agresti
41	**Recensioni bibliografiche.** Autori: Massimiliano Cannata e Laurent Chrzanovski

Vivere OnLife

Autore: Nicola Sotira

Il termine OnLife è un neologismo coniato nel 2013 dal Prof. Luciano Floridi per definire la nuova società digitale. Una parola che sta ad indicare l'intreccio tra la nostra esperienza di vita digitale e fisica (Online e Offline). Un mondo con nuove regole con responsabilità liquide condivise fra strumenti e persone, dove è sempre più impercettibile la distinzione tra reale e virtuale. Un rapporto con le tecnologie scandito dal cambio delle nostre abitudini, come rilevato dal rapporto del CENSIS. Il rapporto sottolinea, infatti, come un italiano su due controlla lo *smartphone* prima di prendere sonno e appena sveglio, mentre uno su quattro non esce di casa senza un *power bank* (una batteria di scorta). Numeri che non ci devono stupire visto che ormai il nostro HUB di ingresso al mondo digitale è rappresentato da questo oggetto che continuiamo, per abitudine, a chiamare telefono. Una metamorfosi digitale che sta cambiando le nostre abitudini e le nostre interfacce, un futuro digitale sul quale si interroga anche ShoShana Zuboff, docente della Harvard Business School e autrice del saggio "Il Capitalismo della sorveglianza". Uno degli interrogativi con la quale l'autrice apre il libro è:

"Potremo chiamare casa il futuro digitale?", una domanda che resta aperta in uno scenario nel quale il mondo digitale prende il sopravvento e l'idea di un futuro prevedibile svanisce pian piano.

Fondamentale diventa, in questa era, il fattore conoscenza sia per quanto concerne il tema della formazione delle nuove generazioni sia per quanto concerne l'utilizzo degli strumenti digitali e sul tema della sicurezza. L'accelerazione del digitale ha messo in evidenza come il problema della sicurezza cyber sia oggi uno dei problemi da mitigare per garantire una transizione di successo. Le istituzioni e le organizzazioni hanno una maggiore probabilità, oggi, di ricevere attacchi di phishing o ransomware e molti dei loro dipendenti e/o clienti non sanno nemmeno che cosa significhino queste due sigle. In un contesto dove l'accesso alle informazioni è illimitato, un numero preoccupante di dipendenti delle organizzazioni non è attrezzato per contrastare il crescente numero di attaccanti che prendono di mira i loro luoghi di lavoro ogni giorno, rappresentando pertanto l'anello debole del sistema. Un programma di formazione continua sulla consapevolezza della cyber-security e sull'uso consapevole delle tecnologie digitali può garantire alle organizzazioni, ed al paese, quella resilienza necessaria alla sopravvivenza in questo dominio digitale. Ovviamente, parliamo di formazione continua poiché gli strumenti di attacco evolvono e gli attaccanti troveranno sempre nuove metodologie per inserirsi nei sistemi e le sfumature potrebbero essere così difficili da comprendere richiedendo capacità sempre aggiornate. I vantaggi di questi programmi sono immediatamente visibili, l'aumento della resilienza organizzativa mitiga il rischio per la sicurezza riducendo l'errore umano e le inefficienze di processo. Vivere OnLife in modo consapevole è il passo per traguardare una trasformazione sempre più a misura di uomini. ■

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.

Educare e sensibilizzare, obiettivi chiave della Fondazione GCSEC

Autore: Elena Mena Agresti, GCSEC

Per chiunque operi nel campo della cyber security, è oggi piuttosto chiaro come la formazione e l'awareness siano indispensabili per garantire un elevato livello di sicurezza dei servizi digitali e delle informazioni aziendali.

Con la digital trasformation e nella protezione dei servizi il ruolo dell'utente è diventato sempre più centrale e se non adeguatamente educato, può diventare l'anello debole ancor più di quanto lo fosse nel passato, a causa della scarsa sensibilità e sensibilizzazione alle tematiche di sicurezza.

BIO

Laureata in Ingegneria Aerospaziale presso l'Università La Sapienza di Roma, opera per la Fondazione GCSEC e il CERT di Poste Italiane. Esperta di compliance, standard internazionali, governancedell'information security, gestione dei rischi, security audit, formazione eawareness, ha partecipato a tavoli tecnici internazionali dell'ISO e OCSE per la revisione e lo sviluppo di standard e linee guida di information security. È stata responsabile scientifico di tre corsi di master in cyber security istituiti nel 2015-2016 con l'Università della Calabria e Poste Italiane eattualmente collabora con numerose università italiane in corsi di cyber security. Ha lavorato presso diverse società di consulenza, tra cui in Booz & Company nella practice Risk, Resilience and Assurance. Membro di Europrivacy e della Oracle Community for Security, è Lead Auditor ISO/IEC 27001:2013 e ISO 22301 e ha conseguito le certificazioni STAR Auditor e ISIPM Project Management.

Se in tempi addietro la sicurezza era concepita soprattutto da un punto di vista perimetrale oggi il perimetro è cambiato. I servizi saranno erogati sempre più tramite app mobile e l'avvento dell'Intelligenza Artificiale, IoT e 5G rivoluzioneranno l'attuale modo di pensare del digitale mettendo l'utente sempre più al centro.

Posto che è inevitabile che gli utenti siano l'anello più debole della catena operativa della cybersecurity è pur vero che possono diventare la prima linea di difesa contro gli attacchi informatici. Fare *awareness* significa fornire agli utenti gli strumenti per comprendere minacce, attacchi e rischi cui sono esposti e di conseguenza elevare il livello di sicurezza dell'azienda. La consapevolezza dei rischi a cui è soggetto il personale e dei comportamenti corretti da adottare può ridurre sostanzialmente il livello di rischio *cyber* dell'organizzazione. Clienti sensibili ai temi della cybersecurity riducono il numero di tentativi di frode andati a buon fine e di conseguenza i danni economici diretti e indiretti per l'organizzazione.

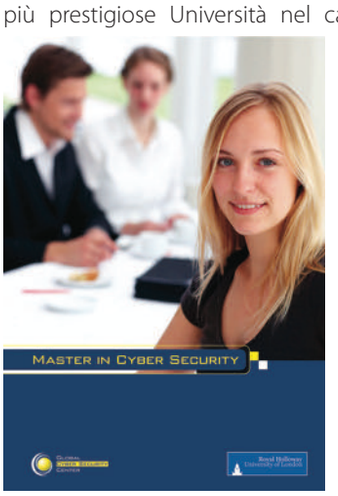
Il tema dell'educazione e della sensibilizzazione purtroppo non riguarda solo gli utenti o il dipendente medio, ma ahimè anche i vertici aziendali, spesso oggetto di attacchi diretti e mirati, così come il personale tecnico della cybersecurity. Per quest'ultimo, da uno studio condotto da GCSEC con l'Università di Oxford, è emerso che molti governi anche tecnologicamente avanzati come l'Australia, il Giappone, il Regno Unito e gli Stati Uniti, vedono l'attuale mancanza di competenze e di professionisti nel mercato del lavoro della cyber security, come una minaccia alla loro sicurezza informatica nazionale.[1]

Per rispondere a queste necessità, alcuni governi hanno definito delle vere e proprie strategie nazionali per elevare il livello di competenze di cyber security a più livelli stanziando anche budget considerevoli come il Regno Unito il cui budget 2011-2016 per l'attuazione dei propri programmi educativi sulla cyber security era pari a £32.8milioni.

Nel suo piccolo la fondazione GCSEC ha concentrato negli ultimi anni tutti i suoi sforzi nello sviluppare, diffondere e condividere conoscenze sulla sicurezza informatica.

Sempre attiva nei programmi di ricerca e di sensibilizzazione dell'UE, GCSEC ha sviluppato progetti di Information Sharing, sicurezza dei Sistemi di Controlli Industriale e delle Smart Grid, programmi educativi nazionali sui temi della cyber security come nel caso del progetto con il governo del Montenegro.

Nel 2012 GCSEC ha portato per la prima volta in Italia il Master of Science in Information Security in collaborazione della Royal Holloway University of London, una delle più prestigiose Università nel campo della sicurezza informatica offrendo ben 12 borse di studio a dirigenti, quadri e funzionari governativi e di organizzazioni private al fine di migliorare le loro conoscenze e competenze sulla sicurezza informatica attraverso un corso riconosciuto a livello internazionale.



Per alimentare le competenze e creare una conoscenza e cultura *"comune"* ha pubblicato i risultati di numerosi suoi studi come *"DNS Health and Security"* in collaborazione con ICANN, *"Condivisione delle informazioni e partenariati pubblico-privato: prospettive e proposte"* in collaborazione con UNICRI, *"Best Practices in Computer Network Defense: Incident Detection and Response"* in collaborazione con la NATO, report sulla sicurezza degli ATM, su case study di APT, blockchain e PSD2 per approfondire e condividere con gli addetti ai lavori tematiche rilevanti nel settore.

Una recente iniziativa di grande successo della fondazione è CERT STAR il programma di incontri a porte chiuse dedicato ai CERT e ai SOC italiani e volto ad alimentare le competenze, promuovere la cooperazione e la condivisione di esperienze. Nel corso degli incontri sono analizzate a livello tecnico operativo le principali tematiche "core" dei team di security quali ad esempio le tecniche di threat hunting, incident prevention e response, intelligence, tutte attività comprensive di esercitazioni pratiche *hands-on* con tool tecnologici.

Il programma 2020 prevede un nuovo format comprensivo di giornate dedicate a cyber challenge come le CTF ***(capture the flag)*** e meeting che si svolgeranno sia a Roma che Milano con uno specifico incontro all'estero per apprendere le best practice, così come le lesson learned, di uno dei più importanti CERT del panorama internazionale.

Attraverso le sue iniziative editoriali quali la rivista Cybersecurity Trends e la newsletter mensile pubblicata in lingua inglese, GCSEC mettere a disposizione di tutti conoscenze, competenze ed esperienze dei vari autori e dà voce anche a realtà di eccellenza. Con contenuti di all'alta qualità, quasi sempre inediti, attrae i suoi lettori anche grazie alla varietà delle tematiche trattate che variano dalle cyber news del momento, ai focus di esperti del settore, dalle nuove minacce vulnerabilità e tecniche d'attacco cyber, a pillole di saggezza per sensibilizzare gli utenti sui comportamenti corretti da seguire.

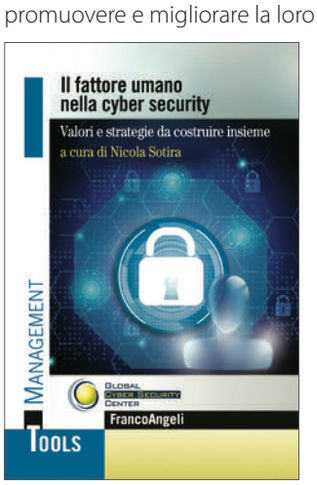
Anche giovani sono sempre stati in primo piano per le attività di awareness. Per loro la Fondazione ha svolto diverse iniziative. Insieme a Poste Italiane e alla Polizia Postale e delle Comunicazioni ha prodotto la versione italiana delle linee guida dell'ITU, l'Unione internazionale delle telecomunicazioni, e in particolare, la *"Guida per la protezione dei bambini nell'uso di Internet"* e la *"Guida per genitori, tutori ed insegnanti per la protezione dei bambini nell'uso di Internet"* con l'obiettivo di stabilire le basi per rendere Internet un luogo migliore e più sicuro per i più piccoli e gli adolescenti.

Sempre con Poste Italiane e la Polizia Postale e delle Comunicazioni ha portato in Italia e tradotto in lingua italiana la mostra *"Eroi e vittime dei Social Media. Dai geroglifici a Facebook"* al fine di sensibilizzare le giovani

generazioni sui rischi legati all'uso scorretto di Internet e dei social media

La mostra illustra, come nel corso degli anni, la comunicazione si sia evoluta e quanto le strategie mediatiche siano state in grado, dai tempi dei geroglifici, passando per l'invenzione della stampa di Gutenberg e alla comunicazione digitale dei giorni nostri, di distruggere l'immagine e la reputazione di un individuo oppure migliorarla.

GCSEC ha svolto anche diversi incontri con adolescenti e scolaresche per risaltare l'importanza sociale di educare le giovani generazioni e mostrare loro gli effetti e le conseguenze dell'uso di Internet e dei social media e per promuovere e migliorare la loro sicurezza online.



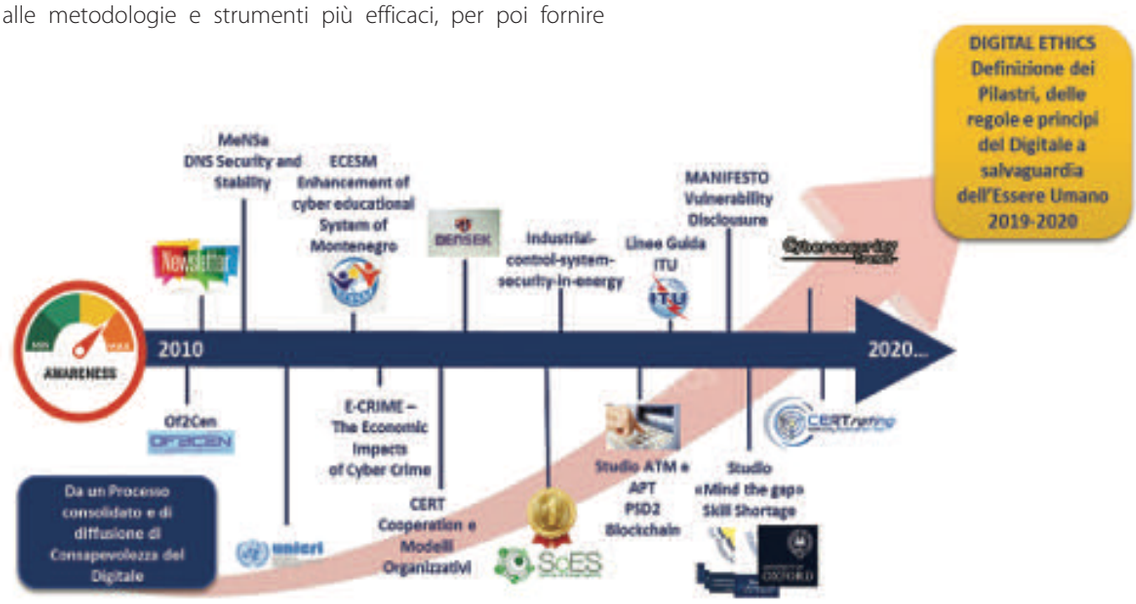
Nei primi mesi del prossimo anno la casa editrice Franco Angeli pubblicherà *"Il fattore umano nella cyber security - Valori e strategie da costruire insieme"*, un manuale operativo della Fondazione GCSEC che intende aiutare chiunque si voglia avvicinare al mondo dell'awareness nel settore della cyber security. I target di riferimento del volume sono molteplici, dai team che operano nell'ambito della tutela aziendale, alle Risorse Umane, alle funzioni di Comunicazione e Formazione, al variegato fronte dei professionisti impegnati a far crescere e a diffondere un'adeguata cultura della prevenzione del rischio. Il libro, che punta ad essere un manuale agile costruito con linguaggio semplice e diretto, racconta con approccio pragmatico l'awareness in ogni suo aspetto.

Dal perché sia necessaria, ai passi da seguire per creare una campagna di successo, alle metodologie e strumenti più efficaci, per poi fornire indicazioni ed esempi concreti sui contenuti da veicolare e sulle tecniche digitali e non digitali da utilizzare per rendere le campagne efficaci. Una sezione speciale è dedicata alle misurazioni delle attività di awareness e alle prospettive future.

Fino ad oggi la GCSEC ha svolto attività di Sensibilizzazione e Consapevolezza ma si è resa conto che per essere ancora più efficaci dovrebbero essere affiancate da un approccio concreto nello sviluppo del digitale per passare da un processo consolidato e di diffusione di consapevolezza ad uno sviluppo etico del digitale.

Per raggiungere questi obiettivi, GCSEC e Sloweb, un'associazione non profit fondata per promuovere l'uso responsabile degli strumenti informatici, del web e delle applicazioni Internet, stanno promuovendo il tema dell'etica digitale; il primo passo per accendere un dibattito costruttivo sull'etica che coinvolga a 360° Istituzioni, Accademia, Aziende e Professionisti con la necessità di definire i principi Etici per una innovazione ed evoluzione che si basi su sicurezza, sostenibilità e privacy. In particolare, la Fondazione GCSEC e Sloweb hanno avviato un progetto sulla definizione e promozione di un Manifesto sull'Etica Digitale. Lo scopo del documento è quello di condividere e sottoscrivere, con organizzazioni pubbliche e private, un impegno solenne sul rispetto dei principi secondo una visione Etica e sull'utilizzo e sviluppo consapevole e responsabile delle tecnologie digitali. ■

1 GCSEC & University of Oxford Centre for Doctoral Training in Cyber Security - "Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions" – 2019. Disponibile al seguente link: https://gcsec.org/wp-content/uploads/2019/02/cyber-ebook-definitivo.pdf



Intervista VIP: Cinquant'anni di Internet a colloquio con Arturo di Corinto

Arturo di Corinto

Autore: Massimiliano Cannata

Igiene cibernetica, è il primo passo per un'efficace awareness e per non tradire la missione originaria della rete

Il 29 ottobre del 1969 avveniva il primo collegamento tra due computer. Mezzo secolo dopo Jaron Lanier, l'inventore della realtà virtuale lancia, in un'intervista a Riccardo Luna apparsa su Repubblica, un allarme molto preciso "dobbiamo aggiustare la Rete. Viviamo in un capitalismo digitale fondato sulla manipolazione delle coscienze praticato con il furto dei dati. Bisogna cambiare il modello di business e rimettere al centro gli utenti che sono il vero motore del mondo futuro". Parliamo di questo anniversario "speciale" con Arturo di Corinto, psicologo cognitivo, esperto di innovazione tecnologica, collaboratore di quotidiani e riviste di settore, svolge un'intensa attività pubblicistica. Docente presso la *Link Campus University* di Roma è abituato a confrontarsi quotidianamente con gli studenti sulle grandi questioni della contemporaneità.

Professore, la Rete si è "guastata" ha ragione Lanier?

Quando si parla di Internet penso si debba parlare di una rivoluzione ampiamente sottovalutata, che ha letteralmente terremotato il nostro modo di vivere, ha cambiato il mondo di organizzare e produrre il lavoro, il volto delle nostre città, ha ridotto la coda agli sportelli, ha "cancellato" alcuni ambiti occupazionali riducendo le "vetrine" dei negozi tradizionali, gli spazi delle botteghe artigiane, fatto sparire le mercerie sotto casa, i tanti negozietti dove facevamo salotto, ha modificato le modalità di relazione e di conoscenza tra gli esseri umani. L'elenco dei cambiamenti potrebbe continuare, però, prima di andare avanti, vorrei sgombrare il campo da un equivoco di fondo.

Approfittiamone subito.

Internet non è il web e il web non è Internet. Internet è la piattaforma di comunicazione che permette ai computer sparsi ai quattro angoli del pianeta di scambiarsi le informazioni che risiedono negli *hard drive*. Come è noto dobbiamo a *Robert Kahn e Vint Cerf*, che all'inizio degli anni ottanta, riuscirono a trovare la formula giusta per aggregare in modo innovativo una famiglia di protocolli costruendo il **TCP/IP**, la creazione della lingua che consente ai computer di "parlarsi" senza che si perdano "pezzi" preziosi di informazione. Ricordiamo che reti di computer esistevano già da molti anni, ma l'utilizzazione del TCP *(trasmission control protocol)* ha consentito un uso massivo di Internet. E' da quel momento che la storia cambia il suo corso.

Eravamo partiti dalla errata identificazione di Internet e Web…

Torno subito sulla questione. Il web, la cui invenzione va attribuita all'ingegnere informatico, *hacker* inglese *Tim Berners-Lee,* è il modo in cui possiamo rappresentare in maniera grafica, multimediale, interattiva i

BIO

Sono uno psicologo cognitivo, insegno all'Università e lavoro come giornalista. Esperto di Internet, nuove tecnologie e comportamenti sociali, mia madre non ha ancora capito che lavoro faccio. Ho cambiato spesso lavoro. Dopo la Rai, la Presidenza del Consiglio dei Ministri, l'Università Sapienza di Roma e la Regione Lazio, ho lavorato per l'Ires-Cgil come ricercatore. Prima di questi incarichi ho lavorato come ricercatore per le Nazioni Unite, l'Isfol, il Censis. Ho anche lavorato come responsabile della comunicazione del Laboratorio Nazionale di Cybersecurity del CINI fino a maggio 2019.

contenuti digitali presenti nei server collegati in Rete. Il *web* è dunque un servizio, quindi una parte di Internet, che per la sua immediatezza e facilità d'uso è diventata una vera e propria *killer application*, il cuore, per dirla in altri termini, di quella rivoluzione oggi al centro del dibattito.

La democratizzazione della conoscenza

Miliardi di utenti popolano questo spazio virtuale, quale motivazione li spinge?

E' il linguaggio ipertestuale (HTML scoperto da Berners-Lee n.d.r.) che consente a una platea che possiamo definire universale, di fruire in maniera facile e immediata, dei documenti elettronici distribuiti tra i vari PC. I progettisti hanno, infatti, concepito il funzionamento del web in maniera analoga al modo in cui funziona il sistema umano di elaborazione delle informazioni. Le tecniche attraverso cui noi gestiamo linguaggio, memoria apprendimento, comunicazione sono state incorporate in questi software, che grazie a degli *escamotage* di carattere psicologico permettono all'utente di comprendere intuitivamente le "istruzioni per l'uso". Pensiamo al *"cestino"*, sul desktop sappiamo tutti a cosa serve nella vita reale, o alle "forbici" presenti nella consolle di Microsoft. E' evidente che l'insieme di questi fattori hanno portato a una democratizzazione dell'informazione e dell'accesso alla conoscenza e alla smaterializzazione di tutta una serie di attività che prima ci obbligavano a uscire di casa e a essere presenti. E' questa la rivoluzione nella rivoluzione, che segna una cruciale e radicale discontinuità rispetto alle epoche passate.

Finalità prettamente militari, secondo molti studiosi, avrebbero fatto da "stato attrattore" dello sviluppo di Internet. Qual è stato l'effettivo peso di questa componente?

Siamo di fronte a un altro "mito" da sfatare. Lo scopo di Internet fin dalla sua origine è quello di rispondere al sogno della biblioteca universale, che si traduce nella possibilità concreta di ottenere liberamente informazioni e conoscenze. La comunità scientifica, utilizzando gli applicativi di questo eccezionale strumento, poteva finalmente "dialogare" senza limiti spazio- temporali, disponendo di un giacimento infinito di *know how*. L'"era dell'accesso", il celebre scritto di Rifkin, comincia così.

L'ibridazione di virtuale e reale è uno degli effetti che tutti sperimentiamo continuamente. Con quali conseguenze?

Si è affermata una nuova categoria dell'essere: *"on life",* è la definizione molto efficace usata da Luciano Floridi che vorrei richiamare. Oggi quello che succede nel mondo on line ha un riflesso nel mondo analogico e viceversa. Le nostre attività sono una commistione di questi due ambiti. Come possiamo dire di vivere nel mondo analogico quando, come risulta dagli ultimi dati, tocchiamo circa 2500 volte al giorno il nostro *smartphone?* Attraverso il digitale ordiniamo sempre più spesso il cibo per la cena, prenotiamo il medico che ci dovrà visitare, e prendiamo appuntamento con una nuova fiamma. E' chiaro che non sono mutate solo le mosse che quotidianamente facciamo, nella dimensione *on life*, è cambiata la scacchiera, come ha ben argomentato Alessandro Baricco (cfr. *The game,* ed. Einaudi n.d.r). Attenzione però a un aspetto.

La ascolto…

Corriamo il rischio di considerare l'accesso alla rete una commodity al pari di altri beni, come l'acqua, finendo col dare con superficialità tutto per scontato. Se l'acqua, bene comune per eccellenza che abbiamo ormai in tutte le case, è vita, l'accesso a Internet ha fatto forse ancora di più, perché ha modificato il nostro modo di pensare. Il fatto che in rete abbiano maggiore successo

i servizi con audio e immagini, non deve stupirci perché sono le modalità primitive di interazione con il mondo, precedenti alla parola, all'alfabeto, alla scrittura. Come ha ben evidenziato il filosofo del linguaggio Raffaele Simone (cfr *La terza fase, forme di sapere che stiamo perdendo, ed. Laterza* n.d.r) siamo passati da una lettura alfabetica a una lettura visuale, un processo sempre più visibile e accentuato con cui dobbiamo imparare a fare i conti.

La perdita della scrittura, un rischio da governare

Non corriamo il rischio di perdere la scrittura, come abilità e come competenza?

Questo pericolo è per il momento scongiurato dal fatto che su Internet inneschiamo le nostre ricerche scrivendo delle parole-chiave. Le cose stanno però cambiando, Google permette di fare le nostre navigazioni con gli assistenti virtuali, con il risultato non ci sarà più bisogno di focalizzare l'attenzione su qualcosa di specifico, assumendo la postura classica che permette la scrittura. Di questo passo non useremo più le mani, ma solo la voce, anche per chiudere le tapparelle e fare i lavori di casa. E' chiaro che il "terremoto", per rimanere alla metafora iniziale, che sta investendo gli *asset* relazionali, i sistemi sociali, economici e politici, provocherà altri scossoni.

I punti "oscuri" della rivoluzione in corso riguardano la sicurezza delle reti. Da regno della libertà siamo passati, nel breve volgere di pochi anni, a doverci misurare con un orizzonte denso di rischi crescenti. Siamo preparati?

I rischi sono connessi alla digitalizzazione di tutte le attività umane. Una volta il delinquente saliva sul balcone e ci entrava in casa, oggi entra nel conto bancario, nel pc, nel telefonino. Allo stesso modo le polemiche e le diversità di opinione si consumavano al bar o nella piazza del paese, oggi tutto avviene sui social. Gli "odiatori" seriali, fenomeno crescente in Rete, si possono scatenare perché l'assenza fisica dell'interlocutore elimina la paura della rappresaglia, inducendo questi soggetti a non avere cautela, pudore, vergogna, quando esprimono opinioni estreme. Sul web interagiamo con persone mai viste e pensiamo che sia permesso tutto. Errore molto grave, perché i reati e le leggi valgono anche su Internet.

La* cyber security *di quali strumenti dispone per arginare i crimini* on line*?

L'eterna lotta tra guardia e ladri si è spostata sul terreno virtuale senza esclusione di colpi. La digitalizzazione del crimine, ha portato allo sviluppo di nuovi strumenti di prevenzione e repressione. Oggi disponiamo di software che ci permettono di stabilire in anticipo la possibilità che si verifichi un evento criminogeno in una certa area della città. Questo è possibile grazie ad algoritmi che masticano dati e che ci danno un tasso di probabilità, secondo delle inferenze statistiche.

Awareness *(sensibilizzazione n.d.r) sembra essere il termine critico, per chi oggi si occupa di sicurezza. Come si declina questo concetto nella quotidianità dei nostri comportamenti?*

Sicurezza informatica e dipendenza sociale e psicologica dalle tecnologia vanno di pari passo. *Awareness* vuol dire avere consapevolezza che gli strumenti vanno tenuti "puliti", da virus e tenuti lontani da ospiti indesiderati. Quello che dobbiamo sviluppare è insomma una coscienza diffusa di IGIENE CIBERNETICA. Una volta ci mettevamo a tavola dopo aver lavato le mani per evitare infezioni e malattie. Lo stesso dobbiamo imparare a fare con i computer che vanno "igienizzati" e tenuti in sicurezza.

La necessità di un'adeguata Igiene cibernetica

Nelle organizzazioni produttive l'"igiene cibernetica" di cui parla, che significato assume?

L'igiene cibernetica si impone prima di tutto nei luoghi di lavoro, perché ormai il 90% delle persone svolge le sue mansioni davanti a un terminale. Un attacco ransomware può bloccare una rete di bancomat mandando in tilt le operazioni di milioni di utenti, la contabilità di un'azienda può essere bloccata da un un'azione di phishing, così come una centrale elettrica piuttosto che un aereoporto. Dobbiamo comprendere che il "gigante tecnologico" fatto di potenza trasmissiva ed elaborativa di cui stiamo celebrando i cinquant'anni ha la fragilità di chi ha i piedi d'argilla. Da qui la necessità di lavorare sul fattore umano, attraverso campagne di *awareness* finalizzate, corsi di formazione, pubblicazioni. Il linguaggio del *gaming* viene per esempio molto utilizzato come strumento di formazione, al fine di imparare le tecniche di difesa dai malfattori digitali, altri metodi si stanno facendo strada a dimostrazione che le aziende stanno rafforzando gli investimenti nell'ambito della cybersecurity.

L'individuo si sta sempre più rilevando come l'anello debole della catena. Furto di dati personali e industria delle* fake news *sono le aree critiche. Stefano Rodotà nei suoi lunghi anni di ricerca e di impegno in qualità di garante sul terreno dei diritti digitali, parlando di necessità di "tutelare il corpo elettronico" aveva per primo intuito il destino complicato della privacy. A che punto siamo su questo delicato fronte?

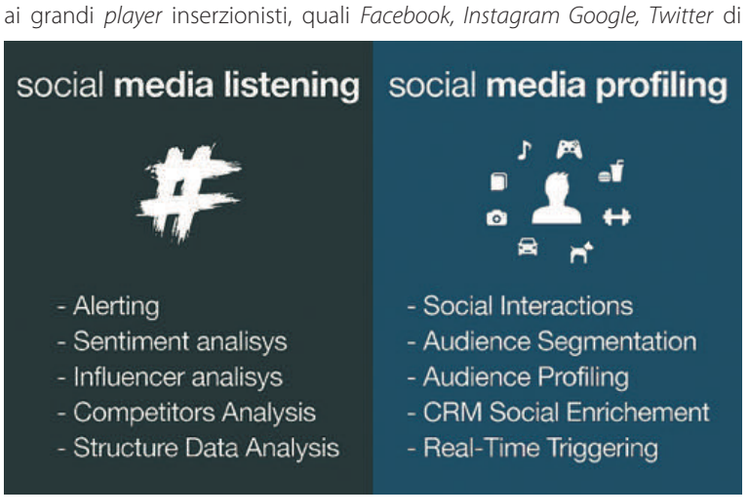
La privacy è la faccia complementare della cyber security. Libertà, autonomia, riservatezza, intimità, la vetrina di Internet mette continuamente

a rischio tutto questo. La privacy è un fatto relazionale, non dipende, come diceva Rodotà, da una tecnologia, né da una legge. Quando chiedo un mutuo in banca, è importante che non lo sappiano gli altri, perché queste informazioni hanno un peso sulla reputazione. Il caso dei social è quello più eclatante. E' lì che mettiamo spesso foto che danno un'immagine alterata di noi stessi. Le conseguenze sul piano del lavoro e della *reputation*, le conosciamo tutti, credo sia inutile insistere.

L'industria delle *fake news*

Soffermiamoci in conclusione sull'industria delle* fake news*, che condiziona sempre di più la vita democratica di intere nazioni. Scenari inquietanti si stanno aprendo, come invertire un trend così pericoloso?

Le *Fake news* sono la testa d'ariete delle campagne di manipolazione delle percezioni. E' un'antica tecnica di guerra che induceva all'errore il generale, il politico, il funzionario facendogli fare delle mosse che avvantaggiavano gli avversari. Uno strumento classico di propaganda, che i russi, ma non solo, conoscevano bene. Interagendo sui social offriamo una mappatura dei nostri gusti e delle nostre preferenze. La profilazione sui social permette ai grandi *player* inserzionisti, quali *Facebook, Instagram Google, Twitter* di proporre quello che siamo più propensi a desiderare. Il motore delle fake news trae così la sua energia, generando un alone di verità creata, che risponde ai nostri gusti e tendenze politiche, costruita con gli algoritmi che elaborano delle informazioni coerenti con le nostre inclinazioni. Questo tipo di condizionamento, che di fatto prosciuga la libertà di ricerca dell'utente è in grado di modificare i nostri comportamenti e di mutare, tra l'altro, l'esito delle competizioni elettorali, come è avvenuto ed è facile prevedere avverrà ancora in diversi paesi.



Difficile trovare dei correttivi. La proposta di legge Marattin che prevede l'obbligo della carta di identità per iscriverci ai social, al fine di limitare il proliferare sul web di notizie false e odiatori seriali, è un correttivo possibile?

Mi permetta di rispondere con una battuta: quando non paghiamo qualcosa ricordiamoci che il prodotto siamo noi. Attenzione dunque ai motori di ricerca e a quei servizi che danno tutto gratis, perché esistono delle valide alternative che a un prezzo sostenibile offrono garanzie all'utente. Nel contempo facciamo pulizia di inutili *app* e di notifiche se desideriamo evitare che altri guardino nel buco della serratura della nostra intimità. Senza un approccio di maggiore consapevolezza, ecco la giusta *awareness cui lei faceva riferimento nella domanda*, saremo allevati come polli da batteria, a disposizione del miglior offerente. Se, invece, ci impegniamo a utilizzare con senso di responsabilità la rete allora potremo contribuire a dare corpo al sogno originario, e si potrà tornare a parlare della rete come di uno strumento che deve fare il bene dell'umanità consentendo alle persone di ritrovarsi e di fare delle cose belle, insieme. ■

Ricevi gratuitamente la newsletter registrandoti sul nostro sito:
www.gcsec.org/newsletter-1

OcchioAlClic!

La campagna di awareness 2019 del CERTFin

OcchioAlClic è la campagna di sensibilizzazione realizzata dal CERTFin sui rischi relativi all'utilizzo dei sistemi di pagamento digitali e sulle buone pratiche da adottare per evitare di incorrervi.

CHI È IL CERTFin?

IlCERTFin – CERT Finanziario Italiano è un'iniziativa pubblico-privata che ha l'obiettivo di fornire un supporto strategico ed operativo al sistema bancario e finanziario in tema di prevenzione e risposta agli attacchi informatici.

È presieduto dall'ABI (Associazione Bancaria Italiana) e da Banca d'Italia ed è operato dal Consorzio ABI Lab. Conta ad oggi 50 aderenti (banche, assicurazioni, centri servizi e infrastrutture di mercato).

L'IMPORTANZA DELL'AWARENESS

Una delle maggiori sfide per la sicurezza informatica è il fattore umano, motivo per il quale le iniziative di cybersecurity awareness giocano un ruolo centrale nel nostro mondo mobile e interconnesso.

Può capitare a tutti di aprire un allegato infetto, fare doppio clic su un URL non sicuro, usare nomi utente e password predefiniti o facili da indovinare, perdere computer o smartphone, divulgare involontariamente informazioni riservate tramite social network, rispondere a e-mail fraudolente… Il mondo virtuale, come il mondo reale, non è esente da insidie.

Sul tema della sensibilizzazione verso la clientela sui rischi del cybercrime le banche italiane sono in prima linea, comunicando attraverso il proprio sito di Internet Banking, attraverso le informative contrattuali o presso le filiali, ma anche promuovendo collaborazioni intersettoriali come il **CERTFin** che, fra i suoi obiettivi, include la realizzazione di iniziative volte ad aumentare la consapevolezza dei clienti in tema di sicurezza informatica e a favorire l'adozione di comportamenti consapevoli nell'utilizzo dei servizi bancari on line.

LA CAMPAGNA OCCHIOalCLIC

Poiché la sicurezza informatica passa anche attraverso la collaborazione dei clienti, abbiamo realizzato, insieme alla Polizia Postale e delle Comunicazioni, la campagna di comunicazione "OcchioalClic" con l'obiettivo di educare sul tema della sicurezza informatica e portare i destinatari ad adottare un atteggiamento virtuoso di buone pratiche nelle operazioni on line.

Per centrare l'obiettivo, abbiamo adottato un approccio comunicativo che sottolineasse la facilità di adottare contromisure e usare i servizi digitali in modo sicuro: OcchioalClic.

Un invito serio, ma al contempo informale, a modificare i propri comportamenti per agire on line in sicurezza: tre semplici parole per catturare l'attenzione dell'utente e sensibilizzarlo.

Con il lancio della campagna lo scorso maggio, il sito del CERTFin si è arricchito della sezione OcchioAlClic: qui è possibile trovare una lista di suggerimenti per scovare e bloccare i tentativi dei malintenzionati on line o per affrontare senza timore la navigazione quotidiana, informazioni sulle più frequenti minacce informatiche e notizie e aggiornamenti sul mondo della sicurezza on line.

I SUGGERIMENTI DI OCCHIOalCLIC

Per operare in rete in modo sicuro quindi è importante FARE ATTENZIONE: gli hacker sono sempre alla ricerca di nuovi modi per fare soldi a nostre spese. Aziende e privati spesso cadono vittime di frodatori che utilizzano tecniche di social engineering o si introducono nei sistemi informatici per rubare o per raccogliere direttamente le informazioni necessarie per la truffa. Le truffe sentimentali, le truffe di investimento sono esempi tipici di come gli hacker possono facilmente giocare sulla psicologia e le percezioni delle persone.

La migliore difesa è la consapevolezza.

Suggerimenti sempre validi:

- Controlla regolarmente i tuoi account on line.
- Controlla regolarmente il tuo conto bancario e segnala eventuali attività sospette alla tua banca.
- Effettua pagamenti on line solo su siti web sicuri (controlla che nella barra degli indirizzi sia presente l'icona di un lucchetto e https) e utilizza connessioni sicure (scegli una rete mobile anziché il wifi pubblico).
- Ricorda che la tua banca non ti chiederà mai informazioni sensibili come le credenziali dell'home banking via telefono o e-mail.
- Se un'offerta sembra troppo bella per essere vera, è molto probabilmente una truffa.
- Conserva i tuoi dati personali al sicuro.
- Fai molta attenzione alle informazioni e alle immagini che condividi sui social network: i truffatori potrebbero usarle per creare un'identità falsa o per architettare una truffa.
- Se ritieni di aver fornito i dettagli del tuo account a un truffatore, contatta immediatamente la tua banca.
- Segnala sempre qualsiasi sospetto di frode alla polizia, anche se non sei rimasto vittima della truffa.

Quindi, è importante seguire alcune semplici regole: cambiare periodicamente la password dell'e-mail, dei social network, dell'internet banking e dei siti per gli acquisti on line; aprire le email solo da indirizzi noti; installare o aggiornare l'antivirus sul proprio computer e smartphone; contenere la diffusione delle informazioni personali on line e usare password diverse per siti diversi.

I CANALI UTILIZZATI

L'area web OcchioAlClic è stata promossa attraverso diversi canali:

- **Stampa quotidiana nazionale**, con uscite sui maggiori quotidiani in area generalista e nella sezione economia/finanza. La presenza su testate di questo tipo ha contribuito a dare autorevolezza all'iniziativa e ha consentito di dare notorietà al progetto presso i referenti delle banche CERTFin.
- **Web Google Display**, con banner realizzati ad hoc e selezione dei posizionamenti su siti di e-commerce, piattaforme di prenotazione on line, siti/blog che trattano il tema dei pagamenti on line. Questo canale ci ha dato la possibilità di comunicare nelle occasioni in cui il destinatario è più sensibile al tema della sicurezza on line.
- **Web posting su Facebook**: un mese di campagna Facebook Ads, con sponsorizzazione dei post presso target definiti in base a specifici interessi (shopping on line, viaggi e vacanze, home banking, carte di credito)., Grazie alla possibilità di segmentare i destinatari in funzione dell'interesse per il tema specifico e dell'attività sulle piattaforme digitali, abbiamo raggiunto in maniera ottimizzata il target.

UN SUCCESSO CONDIVISO

OcchioalClic ha registrato ottimi risultati, con oltre 30 mila visite all'area web durante la campagna. Al successo dell'iniziativa hanno contribuito:

- la Polizia Postale, che ha sposato l'iniziativa incrementando l'autorevolezza dei contenuti promossi e insieme alla Polizia di Stato ha dato visibilità alla campagna tramite social e sito web;
- ABI, che ha dedicato un comunicato stampa all'iniziativa ripreso da diverse agenzie e ha dato visibilità alla campagna tramite il proprio sito web;
- Banca d'Italia e diverse membri del CERTFin, fra cui Poste Italiane, che hanno promosso l'iniziativa tramite social e/o sito web;
- alcune banche del CERTFin che hanno contribuito ad arricchire l'area web OcchioalClic con materiale relativo a iniziative di awareness condotte presso la propria clientela.

WHAT'S NEXT?

Nei prossimi mesi l'area web "OcchioalClic" sarà trasformata stilisticamente per armonizzarsi con il nuovo sito CERTFin, ad oggi in costruzione, e rappresenterà il punto di partenza per un programma di comunicazione articolato negli anni, che si andrà ad arricchire di volta in volta grazie alle future iniziative.

Nella seconda metà del 2020 saremo al lavoro su una nuova campagna di awareness che partirà dalle esigenze e proposte provenienti dalle realtà aderenti e per la quale sarà valutata l'opportunità di realizzare un'iniziativa congiunta di settore.

Per informazioni: comunicazione@certfin.it ■

Intervista VIP Gabriele Faggioli, presidente Clusit, CEO Partners4innovation e Direttore scientifico dell'Osservatorio information security & privacy del Politecnico di Milano

Gabriele Faggioli

Autore: Massimiliano Cannata

La crescita del Cybercrime impone investimenti mirati in tecnologie e formazione del capitale umano

I dati del Rapporto Clusit 2019 parlano di un generale "stallo a livello globale". Sono più di settecento gli attacchi gravi registrati nel primo semestre 2019, con una media mensile di circa 126, in lieve crescita (+1,3%) rispetto allo stesso periodo dell'anno precedente. Pochi spiragli dunque sul fronte della sicurezza cyber. Prof. Faggioli dietro i numeri, si annidano sempre molti significati. Possiamo cercare di individuarli e riassumerli?

Bisogna intanto imparare a leggere con attenzione ed equilibrio ogni proiezione statistica. Dal momento che stanno aumentando le tecnologie disponibili sul mercato, non dobbiamo stupirci se si stanno inevitabilmente ampliando le superfici per attacchi che in futuro saranno potenzialmente più virulenti e si caratterizzeranno per una sempre maggiore capacità di offesa. Fortunatamente non tutti gli attacchi arrivano a buon fine. Nessun apparato può essere definito sicuro in assoluto. Se guardiamo le automobili di trenta anni fa e le confrontiamo con quelle che usiamo oggi, viene spontaneo dire: ma come si faceva una volta a viaggiare con veicoli così insicuri una volta. La storia si ripete e succederà lo stesso con gli *smartphone* e i pc: i nostri figli e nipoti penseranno la stessa identica cosa di noi, guarderanno gli oggetti che abbiamo in mano come insicuri e obsoleti. Quindi nessun allarmismo, bisogna rendersi semplicemente conto che la diffusione degli strumenti digitali sofisticati coincide, in maniera quasi fisiologica, con un innalzamento dei rischi.

Come bisogna attrezzarsi a fronte a un visibile potenziamento della capacità di attacco di reti e sistemi?

Il sistema di difesa che aziende e istituzioni devono mettere in atto deve curare due aspetti: il fattore tecnologico e quello culturale, che vanno di pari passo. L'attenzione mediatica e l'evoluzione normativa hanno creato un generale clima di consapevolezza, fatto positivo che ha

generato investimenti e una maggiore sensibilità delle aziende verso queste tematiche.

Nel Rapporto emerge il dato relativo al* cybercrime*, che rappresenta l'85% degli attacchi a livello globale con un trend in ulteriore crescita e un incremento pari all'8,3% nell'ultimo anno. Per quale ragione questa modalità risulta la più diffusa?

Si tratta di una tipologia di attacco compiuta allo scopo di estorcere denaro alle vittime o di sottrarre informazioni per ricavarne denaro. Questa modalità di aggressione colpisce un numero elevato di persone, non si presenta molto virulenta, generando la maggior parte dei danni a livello globale. Chiara la strategia di questi attaccanti: mantenere un profilo relativamente basso per poter continuare ad agire senza attirare troppo l'attenzione.

TECNICHE DI ATTACCO PER TIPOLOGIA	2014	2015	2016	2017	2018	2018 su 2017	Trend
Malware	127	106	229	446	585	31,2%	↗
Unknown	199	232	338	277	408	47,3%	↑
Known Vulnerabilities / Misconfig.	195	184	136	127	177	39,4%	↗
Phishing / Social Engineering	4	6	76	102	160	56,9%	↑
Multiple Techniques / APT	60	104	59	63	98	55,6%	↑
Account Cracking	86	91	46	52	56	7,7%	↗
DDoS	81	101	115	38	38	0,0%	=
0-day	8	3	13	12	20	66,7%	↑
Phone Hacking	3	1	3	3	9	200,0%	↑
SQL Injection	110	184	35	7	1	-85,7%	↓

Lo studio invita a non sottovalutare alcune "attività criminali spicciole", meno eclatanti ma non per questo trascurabili. A cosa si riferiscono gli esperti Clusit?

A una rete di microfenomeni molto diffusa, come le quotidiane campagne mirate a compiere truffe ed estorsioni realizzate tramite *phishing* e *ransomware,* che hanno colpito moltissime organizzazioni e tanti cittadini italiani. Il trend di crescita che riguarda queste tipologie nel triennio 2017-2019 è una spia molto eloquente che non ha bisogno di ulteriori commenti.

Dal vostro osservatorio come giudicate il livello di investimenti in* cyber security *da parte delle aziende italiane?

Le grandi aziende oramai da alcuni anni considerano la sicurezza una priorità come dimostrano gli investimenti crescenti. Diversa la situazione per quanto concerne le PMI che non dispongono delle stesse risorse e della PA, che presenta un sistema molto articolato e complesso e che sta progressivamente affrontando la transizione al digitale che comporta, un "salto" di visione e di cultura, sia in termini strutturali che organizzativi che saranno decisivi nel futuro.

La "logica industriale" delle cyber minacce

Negli ultimi tempi gli attacchi hanno assunto una "logica industriale", significa che la figura dell'hacker abile e solitario "smanettatore" verte al tramonto?

Vuol dire che esiste una forte costruzione di sistemi di malavita organizzata sul piano industriale che mettono in atto attacchi su scala planetaria. Stiamo parlano di realtà strutturate che ovviamente nulla hanno a che fare con iniziative sporadiche e isolate, che rispondono a tutt'altre esigenze.

Quali sono i target più vulnerabili, alla luce dell'evoluzione della macchina del cybercrimine, che Lei ha fin qui tratteggiato?

Non ci sono più zone franche. Tutti sono ormai diventati bersagli, proprio in virtù del fatto che gli attaccanti sono diventati sempre più aggressivi ed organizzati e possono condurre operazioni su scala sempre maggiore secondo quella "logica industriale" cui lei faceva riferimento prima. Vi sono comunque delle peculiarità. Il settore bancario che fa ovviamente gola per i depositi, le infrastrutture critiche, bersaglio di azioni criminali che intendono creare distruzione e disagio nella popolazione. Discorso a parte merita la sanità che ha subito da gennaio a giugno 2019 un aumento degli attacchi del 31%, non era mai successo dal 2011 anno della pubblicazione del nostro Rapporto. 97 attacchi registrati a livello globale contro strutture sanitarie, è un numero eclatante, che non può passare inosservato. Particolarmente colpita, nei primi sei mesi del 2019, la categoria *Online Services / Cloud*, verso la quale sono stati perpetrati il 14% degli attacchi, con una crescita quasi del cinquanta per cento rispetto all'anno scorso. In questo caso sono i dati, il vero "tesoro" della nuova economia che interessa ai criminali.

BIO

Gabriele Faggioli, legale, è amministratore delegato di Partners4innovation S.r.l. (a Digital360 Company di cui è socio e amministratore). È Presidente del Clusit (Associazione Italiana per la Sicurezza Informatica). È Responsabile Scientifico dell'Osservatorio Security&Privacy del Politecnico di Milano. È Adjunct Professor del MIP – Politecnico di Milano. È membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. E' specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amminstrativa degli enti e nel diritto dell'editoria e del markerting. Ha pubblicato diversi libri fra cui, da ultimo, "I contratti per l'acquisto di servizi informatici" (Franco Angeli), "Computer Forensics" (Apogeo), "Privacy per posta elettronica e internet in azienda" (Cesi Multimedia) oltre ad innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni negli scorsi anni.

Formazione e *awareness*: ecco lo snodo critico

Secondo opinione diffusa non solo nell'ambito degli addetti ai lavori, rimane il fattore umano l'anello debole di un sistema digitale potente e fragile. Quali interventi vanno progettati sul fronte della* security awareness*?

Alla base va affrontato il tema della cultura dell'utilizzazione dell'informatica, a cominciare dalle scuole primarie. I nostri bambini utilizzano *devices* sofisticati già a 4 5 anni, bisogna cominciare presto a far conoscere i rischi sottostanti. Vi è poi un aspetto che attiene all'esempio e allo spirito di emulazione. Non possiamo proibire di usare il cellulare ai nostri figli, se poi quando siamo al volante siamo i primi a violare le norme di sicurezza, usando il telefonino in maniera impropria e pericolosa. Sul fronte delle aziende va detto che bisogna programmare attività formative e di *awareness* non semplicemente per adempiere a una norma, annegando tutto nel "legalese" o nel "burocratese". Occorre utilizzare modelli di comunicazione più smart, e verificare che si inneschi un vero processo di apprendimento. Vanno trasmessi concetti essenziali, senza ripercorrere errori e stilemi del passato, che non sono più coinvolgenti per un target, come quello aziendale, che ha sempre meno tempo e spazi da dedicare alla concentrazione e allo studio molto limitati.

L'università può avere un ruolo, interfacciandosi con la scuola e le aziende?

Lo può avere e direi che lo ha già. Stanno nascendo corsi di laurea focalizzati sulla sicurezza informatica.

VITTIME PER TIPOLOGIA	2014	2015	2016	2017	2018	2018 su 2017	Trend
Gov - Mil - LEAs – Intel	213	223	220	179	252	40,8%	↗
Multiple targets	-	-	49	222	304	36,9%	↗
Health	32	36	73	80	159	98,8%	↑
Banking / Finance	50	64	105	117	156	33,3%	↗
Online Services / Cloud	103	187	179	95	129	35,8%	↗
Research – Education	54	82	55	71	110	54,9%	↑
Software / Hardware Vendor	44	55	56	68	109	60,3%	↑
Entertainment / News	77	138	131	115	102	-11,3%	↘
Critical Infrastructures	13	33	38	40	57	42,5%	↗
Hospitability	-	39	33	34	45	32,4%	↗
GDO / Retail	20	17	29	24	39	62,5%	↑
Others	172	51	38	40	30	-25,0%	↘
Org / ONG	47	46	13	8	18	125,0%	↑
Gov. Contractors / Consulting	13	8	7	6	14	133,3%	↑
Telco	18	18	14	13	11	-15,4%	↘
Automotive	3	5	4	4	9	125,0%	↑
Security Industry	2	3	0	11	4	-63,6%	↓
Religion	7	5	6	0	3	-	↗
Chemical / Medical	5	2	0	0	1	-	↗
TOTALE / MEDIA VARIAZIONI	873	1012	1050	1127	1552		

Anche l'informazione deve fare la sua parte perché si possa diffondere una consapevolezza diffusa sulla necessità di difendere il valore della sicurezza, che rappresenta una delle grandi questioni del nostro tempo. ■

Tecnologia e utenti uniti nel contrasto al phishing

Autore: Roberto Cantarini, Atinet

Il phishing è il metodo principale di accesso nel 91% dei cyber-attacchi di tutto il mondo e molte violazioni di alto profilo sono riconducibili a un singolo tentativo di phishing coronato da successo.

Il phishing è un tentativo di frode messo in pratica attraverso un'email o un sito Web che ha come unico scopo quello di carpire informazioni riservate e sensibili quali, ad esempio, username, password, codici di accesso, numeri del conto corrente o dati della carta di credito. Non a caso *phishing* deriva dal termine inglese *fishing* che significa, per l'appunto, *pescare*.

La verità, è che non importa quanto le barriere perimetrali siano aggiornate, le e-mail malevole troveranno sempre una nuova via per arrivare alle mailbox di destinazione.

In effetti, una recente ricerca di Cofense™ ha osservato che il 90% di tutte le minacce di phishing (malware, Credenziali di phishing, e-mail commerciali e truffe) sono state trovate in ambienti che utilizzano Secure Email Gateway. Nonostante investimenti record, il numero di violazioni riconducibili ad attacchi di phishing continua a crescere.

È ovvio che la tecnologia da sola non può risolvere il problema.

- Quando la tecnologia fallisce, gli utenti costituiscono l'ultima difesa per proteggersi dall'attacco subito
- Trasformare ogni dipendente in un sensore umano altamente vigile.
- La semplice segnalazione di una email come sospetta, aiuta il team del SOC a disattivare gli attacchi in minuti, non mesi.

Il compito dell'azienda è quello di offrire, un programma di formazione continua e di consapevolezza in tutta l'organizzazione con particolare attenzione agli utenti VIP. Non a caso le tecniche di phishing sono maggiormente focalizzate su questa tipologia di utenti.

I dirigenti sono fallibili quanto i loro dipendenti, ma un passo falso nell'ambito della sicurezza da parte di un business leader può provocare conseguenze molto più gravi.

BIO

Ing. Roberto Cantarini, IT Consultant della Atinet S.r.l.,System integrator specializzato in soluzioni di Cyber Security. Lavora nel settore della sicurezza informatica dal 2007, maturando esperienza in diversi ambiti dell'IT. Attualmente è il Project Manager per i progetti relativi all'implementazione della piattaforma di formazione sulla consapevolezza del phishing, prevenzione e risposta agli incidenti, Cofense PhishMe, Cofense Triage/Vision presso realtà italiane di livello enterprise. Si occupa inoltre di implementare soluzioni di Enterprise Data Loss Prevention (DLP) & Device Control e prodotti di IRM (Information Rights Management) presso numerose aziende dei più diversi settori e dimensioni. Affianca alle sue attività, quella di supporto alla configurazione di piattaforme di analisi e monitoraggio della rete al fine di offrire visibilità di contesto per operazioni IT mission-critical.

E' essenziale quindi istruire i dipendenti a riconoscere, evitare e segnalare i vari tipi di attacchi di phishing.

Uno strumento molto utile sono le piattaforme di simulazione che mediante esercitazioni inviano "finte" e-mail di phishing al personale dell'azienda, il cui scopo è appunto, quello di insegnare a riconoscere email malevole e in generale attacchi più complessi.

Di seguiti i 5 passi fondamentali all'implementazione di una corretta campagna di simulazione e relativo e-learning, mirati ad una riduzione del rischio e a promuovere il comportamento desiderato quando una vera campagna di attacco colpisce.

1 ESSERE APERTI E TRASPARENTI SUL PROGRAMMA

Quando ci si imbatte in programmi di simulazione di phishing è essenziale per essere trasparenti con gli utenti sulle ragioni della sua esistenza, e i risultati desiderati. E' essenziale che gli utenti finali comprendano le finalità del programma di simulazione di phishing. Il messaggio percepito dall'utente non deve essere "l'azienda sta cercando di ingannarmi," ma bensì deve essere positivo, orientato al desiderio umano di aiutare ed essere partecipe dell'azienda. È questo sentimento positivo che può essere sfruttato e nutrito da professionisti di sensibilizzazione alla sicurezza per aumentare l'impegno del programma e il successo complessivo.

2 DEFINIRE I RISULTATI DESIDERATI

Il phishing continua ad evolversi ad un ritmo rapido. Nuove tattiche e tecniche di minaccia di phishing emergono quasi quotidianamente.

L'azione di un utente di eliminare un messaggio "sospetto" di posta elettronica fornisce protezione a quest'ultimo, ma non aiuta a proteggere l'organizzazione nel suo complesso. Segnalando l'e-mail sospetta, il SOC Team può ottenere la visibilità necessaria e rispondere in modo appropriato alla minaccia.

L'obiettivo primario dei programmi di simulazione di phishing deve essere quello di mantenere i rischi bene impressi nelle menti degli utenti, in modo da essere in grado di riconoscere tempestivamente le nuove ed emergenti minacce.

Pertanto, il risultato desiderato nei programmi di simulazione del phishing dovrebbe essere quello di incoraggiare la segnalazione da parte dell'utente finale di e-mail sospette. La percentuale di rapporti di simulazione è un indicatore inequivocabile del successo del programma - dopo tutto, fare clic sul pulsante «Segnala phishing» è un'azione consapevole e deliberata.

Come un atleta si allena a gareggiare, gli utenti dovrebbero essere seguire la formazione per far sì che rispondano al meglio, in una situazione di attacco reale.

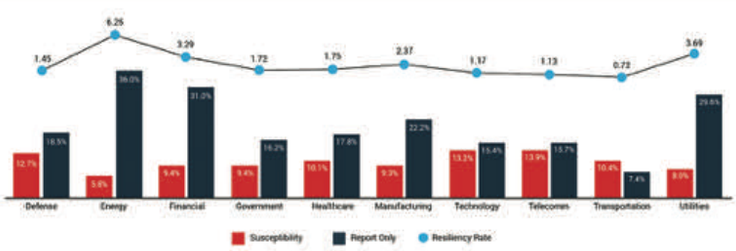
3 IMPOSTARE E MISURARE LE CORRETTE METRICHE

Quando vengono condotti «test» di phishing, la misurazione è guidata dalla mentalità "pass or fail" e viene fissata una soglia in base alla suscettibilità o alla percentuale di clic. **Tuttavia, la percentuale di clic è una metrica intrinsecamente inaffidabile**. Molti altri fattori influenzano l'affidabilità della percentuale di clic come metrica isolata per misurare il rischio effettivo.

Gli utenti hanno ricevuto l'email nella loro casella di posta? Hanno effettivamente letto l'e-mail ? quando l'hanno ricevuta? La decisione di non cliccare su un collegamento o non aprire un allegato, è stata un scelta conscia o di riflesso?

Per Misurare l'efficacia del programma e comprendere l'impatto che sta avendo sulla riduzione del rischio, è necessario guardare oltre la percentuale di clic e misurare i rapporti e la **resilienza**.

La resilienza al phishing viene misurata dividendo il numero di utenti che segnalano una simulazione per il numero degli utenti che hanno effettivamente cliccato. Ad esempio, se in una simulazione, 100 utenti fanno clic su un collegamento, ma soltanto 50 lo segnalano, il punteggio di resilienza è 0.5.



Immaginiamo questo comportamento in una situazione di attacco reale: Al SOC Team viene data visibilità di minacce di cui probabilmente erano ignari; quindi il Team preposto alla sensibilizzazione della sicurezza può legittimamente promuovere il fatto che il loro programma di sensibilizzazione ha veramente ridotto il rischio di minacce.

Quindi, piuttosto che misurare la percentuale di clic, misurare i rapporti e calcolare la resilienza, senza comunque trascurare altre metriche come ad esempio tempo di segnalazione, velocità con cui l'utente segnala l'email di simulazione dopo averla ricevuto.

Quando si dispone di metriche di simulazione affidabili incentrate sui rapporti di e-mail sospette e resilienza al phishing, è possibile combinarle con metriche più ampie per un quadro più completo riduzione del rischio.

Ciò fornisce una visione completa di come i programmi di simulazione di phishing stanno aiutando attivamente l'organizzazione per una migliore difesa dagli attacchi di phishing.

4 FOCALIZZARE LE MINACCE REALI

La maggior parte delle organizzazioni ha la possibilità di eseguire un numero limitato di campagne di simulazione nell'anno. Pertanto ogni

campagna deve produrre un forte contributo alla riduzione del rischio da attacchi. Tutte le piattaforme di simulazione di phishing degne di nota forniscono ampie librerie di modelli di e-mail su cui basare campagne di simulazione.

La scelta di una campagna a caso dimostra una mancanza di comprensione di come aumentare capacità di resistenza agli attacchi di phishing.

Cosa ci aspettiamo dagli utenti quando viene avviata una campagna di simulazione contro il phishing?

a) si avvisino a vicenda della minaccia, suggerendo ai loro colleghi di non fare clic.

b) rimanere in silenzio?

La risposta corretta è a). Infatti i programmi di simulazione devono condizionare gli utenti a comportarsi correttamente nel caso di una situazione di attacco reale. Una risposta di tipo b) suggerisce di rivalutare l'obiettivo della campagna, poiché non è ottimizzata per bloccare attacchi reali.

I programmi di simulazione devono basarsi sull'evolversi tattiche degli attori delle minacce, sull' impatto il settore o posizione degli utenti e sulle minacce specifiche che la tua organizzazione sta affrontando. **Quando la segnalazione delle minacce diventa il risultato principale delle simulazioni, quel comportamento sarà valido anche quando le minacce saranno reali**.

Le email segnalate forniscono una preziosa fonte di informazioni per le successive campagne. Di conseguenza il team preposto alla Security Awareness può migliorare la pertinenza dei programmi di simulazione di phishing garantendo che abbiano un alto grado di attenzione sul tipo di minacce effettivamente ricevute. Avendo più utenti finali che segnalano minacce, si avrà anche una riduzione del carico di lavoro del SOC Team, riducendo inoltre il tempo medio di reazione alla minaccia e successiva Remediation.

5 ANALISI, COMUNICAZIONE, RIPRODUZIONE

Quando si analizzano i risultati di una campagna, si devono identificare le aree in cui è possibile apportare miglioramenti alla resilienza. In molti casi, il comportamento degli utenti alle simulazioni di phishing è rappresentato da una tipica curva a campana.

I programmi dovrebbero anche mirare ad accogliere valori anomali nella curva; appropriati e riconoscimenti per quelli che dimostrano sempre il comportamento desiderato incoraggerà gli altri a fare lo stesso. Allo stesso tempo occorre prendere in considerazione misure appropriate per ridurre i rischi associati a quelli che fanno clic spesso e non segnalano mai.

Per massimizzare le attività formative e consentire ai dipendenti di fornire un contributo fattivo al contrasto del fenomeno spesso le piattaforme di simulazione sono combinate con altri strumenti quali quelli volti a segnalare in tempo reale attacchi di phishing potenzialmente malevoli.

Attraverso un semplice click le segnalazioni degli utenti vengono quindi inviate al SOC aziendale per un'analisi ai fini della sicurezza e per le operazioni di incident response.

Altre funzionalità offrono al personale addetto all'incident response la visibilità e i sistemi di analitica necessari per velocizzare l'elaborazione e la risposta a minacce di phishing segnalate dai dipendenti e diminuire il rischio di violazioni per la sua azienda.

L'insieme di tutti questi strumenti non solo forma i dipendenti a individuare e segnalare le minacce ma anche a migliorare le attività di response.

La piattaforma Cofense™

Cosa si ottiene quando si combinano, un'intelligence contro gli attacchi affidata ai dipendenti con le migliori tecnologie di incident response del settore? Una difesa completa, collettiva e basata sulla collaborazione contro i cyber-attacchi via mail.

Le soluzioni CofenseTM, proposte in Italia da Atinet s.r.l, system integrator specializzato in progetti di cyber-security, anticipano e neutralizzano il ciclo di attacco nella fase delivery, innescando automazione e orchestrazione a livello dell'intera azienda. Ora è possibile respingere gli attacchi in corso e prevenirne eventuali.

Rispondere rapidamente a minacce come spear-phishing, ransomware, malware e compromissione delle caselle di posta aziendali. Tutto questo COFENSE. ■

Intervista VIP a Gianni Baroni, A.D. Daman Group e Cyber Guru S.R.L.

Gianni Baroni

Autore: Massimiliano Cannata

Il valore strategico della security awareness

"Nostro compito è quello di selezionare sul mercato tecnologie all'avanguardia per alzare i livelli di protezione degli asset aziendali. Abbiamo creato un sistema integrato di e-learning (*Cyber Guru* il nome della piattaforma n.d.r) focalizzato sulla *Cyber Security Awareness* per venire incontro a un'esigenza di mercato molto precisa: le aziende investono fior di quattrini in cyber security, per questo si dotano di software sofisticati, che però *hacker* molto abili con tecniche semplici e costi bassi riescono a manomettere con facilità, violando reti e sistemi. Per combattere questa guerra asimmetrica non abbiamo altre soluzioni: bisogna rendere gli individui e le organizzazioni sempre più consapevoli delle minacce che incombono sui processi di trasformazione digitale".

Gianni Baroni AD di *Daman Group* da anni lavora nel campo dell'innovazione. Con i suoi collaboratori affronta ogni giorno la sfida globale della sicurezza informatica, considerata ormai una priorità nell'agenda strategica di istituzioni e aziende.

BIO

Gianni Baroni è l'amministratore delegato del Gruppo Daman. Fondato nel 2003 proprio dall'iniziativa di Gianni, il Gruppo Daman è una realtà che ha la missione di aiutare le organizzazioni italiane pubbliche e private a incrementare il livello di protezione nei confronti del Cyber Crime.
In questi ultimi anni, Gianni Baroni si è dedicato al tema della Cyber Security Awareness, e da una sua iniziativa, nel 2017, è nata la linea di prodotti Cyber Guru, con lo scopo di diffondere all'interno delle organizzazioni la cultura della Cyber Security, trasformando dipendenti e collaboratori nella prima linea di difesa contro il Cyber Crime.

Baroni, la domanda di sicurezza che arriva dal mondo delle organizzazioni produttive si fa sempre più diffusa e pressante. Quali contromisure occorre mettere in campo?

Cyber Guru nasce dalla necessità di reagire con efficacia alle minacce e intrusioni che vengono portate su una superficie d'attacco (*attack surface* si definisce nel gergo tecnico n.d.r.) molto ampia ed esposta a incursioni e violazioni. Quel che è più grave è che sono gli utenti e i dipendenti l'anello debole della "trincea" virtuale, perché inconsapevolmente diventano alleati degli hacker. Basta poco perché succeda, è sufficiente cliccare su un link insidioso o non usare le dovute accortezze nell'aprire una mail o nell'uso del proprio cellulare.

Il deficit che lei denuncia è, dunque, di natura soprattutto educativa?

Il gap educativo esiste, ma attenzione educare in senso generico non basta. Possiamo, infatti, preoccuparci come fanno tutte le organizzazioni, di inviare delle mail dettagliate e complete sulle policy da adottare, ma se ci fermiamo a questo *step* non otterremo gli effetti sperati. Bisogna modificare i comportamenti quotidiani, per marcare una svolta decisiva.

E-learning e nuovi linguaggi

Quello che lei dice presuppone un cambiamento nel modo di progettare e attuare la formazione. Obiettivo non certo facile…

Non facile come lei dice, ma aggiungerei lo stesso che è imprescindibile. Tenuto conto che non è praticabile alcun progetto di formazione in aula, abbiamo progettato una piattaforma e-learning particolarmente innovativa, anche con la collaborazione *dell'Università di Roma Tre*. Teniamo conto che in genere i livelli di *retention* per iniziative del genere non superano il 10-12% troppo poco per questioni - in chiave come la sicurezza.

Come avete fatto a superare l'*impasse*?

Il nostro progetto, in realtà aziendali come BNL dove lo abbiamo implementato, ha superato la soglia dell'80% di *retention*. Il segreto è contenuto in una parola: empatia.

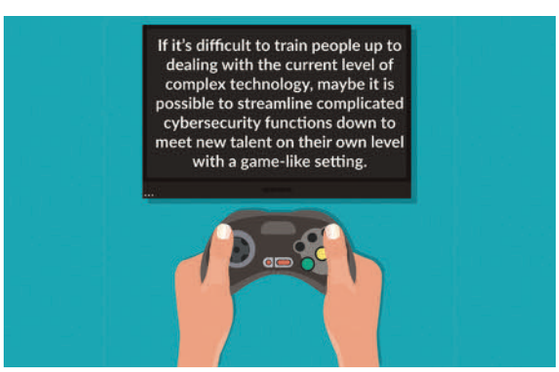
I nostri corsi sono ritagliati a misura di utente e sono tenuti da attori protagonisti che, con linguaggio semplice e coinvolgente entrano in dialogo con ciascun dipendente. Le questioni che vengono trattate nel corso delle lezioni, toccano argomenti personali inerenti la sicurezza. Solo imparando a proteggere i propri file e i propri contenuti on line, si impara a trattare con la massima cura e attenzione il patrimonio di know-how tangibile e intangibile dell'azienda cui si appartiene.

Una componente non trascurabile riguarda l'utilizzazione del* gaming. *Può spiegare di che cosa si tratta?

La *gamification*, così viene definita dagli addetti ai lavori, è un metodo molto efficace di semplificazione del linguaggio e di attrazione del giocatore-utente. Quando si partecipa a un momento di formazione, i nostri appuntamenti sono molti vivaci ed estremamente sintetici, si deve creare una giusta competizione tra i gruppi. Attribuendo un punteggio per ogni risposta esatta, noi premiamo il team di lavoro. Questo consente di strutturare un processo che deve durare nel tempo. Cyber Guru, con cadenza mensile, propone corsi e tematiche sempre diversi, allargando lo sguardo alle grandi questioni del nostro tempo: dall'e-commerce, ai social, al fenomeno delle fake news, al centro della cronaca in questi ultimi tempi.

Non si corre così il rischio di perdere di vista obiettivi più stringenti e concreti?

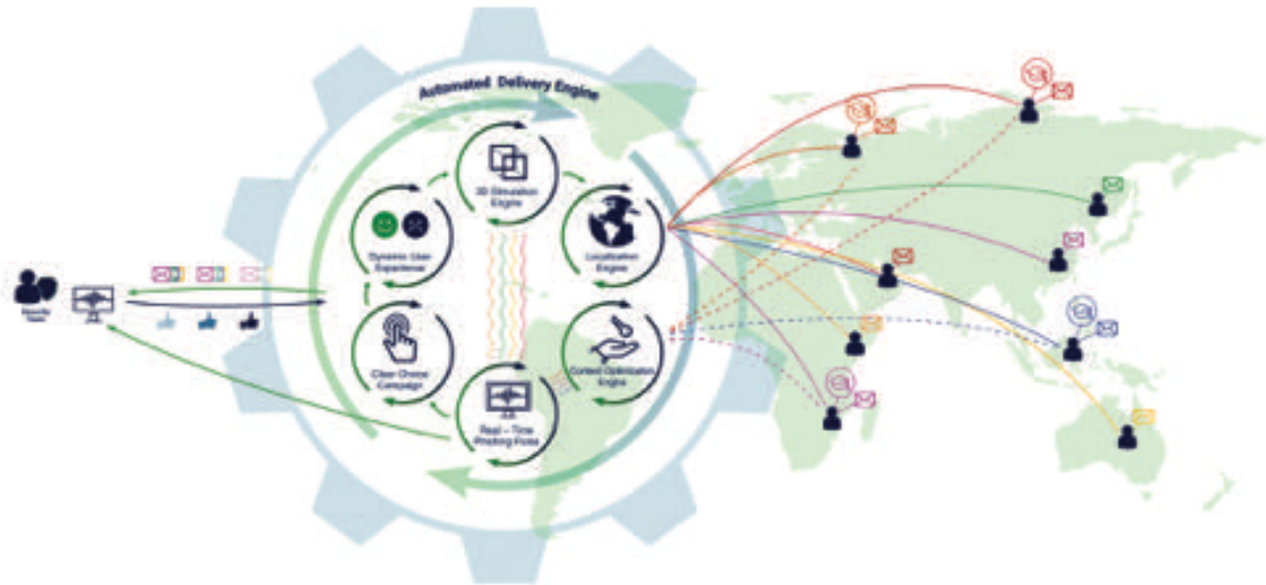
Al contrario, è invece questa la strada che può portare a individuare l'azione subdola degli hacker che utilizzano strumenti, quali i social, come cavallo di troia per violare la privacy degli utenti ed entrare nei sistemi aziendali.



L'efficacia dell'innovazione di sistema

E' corretto definire Cyber Guru, come un'innovazione di sistema?

Direi che è appropriato. ***Cyber Guru Awareness*** è una piattaforma che va a integrarsi con ***Cyber Guru Phishing***, soluzione molto originale e avanzata, che consente, tramite delle simulazioni, di "allenarsi" e di **diminuire i tempi di reazione e di risposta** in caso di attacchi di questa tipologia. La formazione viene attuata tramite rilascio di e-mail progressive, coerenti con il livello di abilità raggiunta dall'utente. Nel corso del tempo gli utenti, sottoposti a periodici training individuali, affinano la loro capacità di analisi a fronte delle violazioni. L'evoluzione della qualità di risposta e della performance da parte di ogni attore dell'organizzazione, rende, così, più difficile e soprattutto più costosa ogni iniziativa



da parte dei cyber criminali. Il nostro obiettivo finale, che poi corrisponde alla "visione" che sorregge l'intero investimento in termini di professionalità e di know-how, che abbiamo messo in campo, è molto chiaro: alzare l'asticella per rendere più difficile, o se si vuole meno probabile, l'azione degli attaccanti.

Cyber Guru da progetto si è tramutata in un'azienda. Si tratta di una best practices replicabile?

Abbiamo una mission molto chiara: produzione e sviluppo di piattaforme e learning da sperimentare in tutt'Europa. La direttiva NIS, come è noto, prescrive a livello Europeo l'obbligo di attuazione di un percorso di *cyber security training* per tutta la forza lavoro che opera in aziende strategiche. L'urgenza oltre che l'attualità di un tema come l'awareness appare molto chiara. Questo non deve portarci a sottovalutare un altro target molto importante.

Quale?

Quello rappresentato dalle PMI, che sono sempre più interessate e motivate ad acquisire competenze in questo delicato ambito. Piattaforme come Cyber Guru consentono una partecipazione universale al progetto, in virtù di costi che sono assolutamente sostenibili. Con un cappuccino al mese, mi passi l'immagine, è possible avviare un affascinante, oltre che utile, percorso di studi. Ripeto spesso l'archetipo che fa da polo attrattore della nostra attività

Vuole in conclusione ricordarlo anche ai lettori di* Cybersecurity Trends*?

Il nostro archetipo è rappresentato dal signor Mario e dalla signora Maria, utenti normali alle prese con la "giostra multimediale" che fa ormai parte del nostro quotidiano e che segna la nostra dimensione on life: telefonino, smartphone, smart tv, una tastiera digitale bellissima ma anche fragilissima, che va maneggiata con cura, perché la nostra vita e soprattutto i nostri affetti e segreti familiari, ma anche lavorativi, passano sulle rotte virtuali. In virtù di quello che ho cercato di spiegare nel corso della conversazione, credo che conoscenza, consapevolezza e responsabilità debbano essere i valori guida dei nostri comportamenti pubblici e privati, in ogni momento della giornata. Se impariamo a ricordarcelo, avremo fatto un importante passo avanti. ■

L'importanza dell'Awareness per la Sicurezza Informatica: il progetto CyberReadiness.IT

Autori: Marco Angelini, Claudio Ciccotelli

Cybersecurity e "fattore umano"

Il panorama attuale della sicurezza informatica affianca ad attacchi estremamente sofisticati, portati ad obiettivi difesi attraverso meccanismi di protezione altamente avanzati, ad un forte uso (e riuso) di attacchi non particolarmente evoluti, eventualmente replicabili con il lancio di semplici script e aventi come obiettivo il raggiungimento del più ampio numero di vittime. In questo scenario, il cyber-crime, come riportato nel rapporto Clusit 2019 [1], è in continuo aumento e si basa esattamente su questa seconda categoria di attacco, a diffusione sempre più ampia. Un fattore critico nella percentuale di successo di questi attacchi, in entrambi gli scenari, è costituito dal fattore umano. Difatti, nel secondo caso la mancanza di consapevolezza in tema di sicurezza informatica porta la vittima di un attacco ad assumere comportamenti errati in termini di postura cyber, con ripercussioni dirette sullo stesso (perdita di denaro, compromissione di confidenzialità, etc…).

Anche nel primo caso, la mancanza di consapevolezza può avere un effetto sul grado di successo di un attacco, rendendo ad esempio meno efficaci le contromisure tecnologiche adottate a fronte di un loro errato o completamente assente utilizzo, o alla ricerca di metodi per superare le barriere spesso imposte da vincoli di sicurezza che mal si conciliano o addirittura risultano incompatibili con i vincoli imposti dalla produttività, per finire ad una sottovalutazione della minaccia, il tutto in base al ruolo ricoperto dall'individuo all'interno dell'organizzazione.

Il "fattore umano" è comunemente considerato l'anello più debole della catena di sicurezza informatica di un'organizzazione, ed una percentuale significativa di aziende ha implementato programmi di awareness e readiness per far fronte a questa vulnerabilità. Tuttavia, la natura aperta di queste campagne, e l'impossibilità o la difficoltà di avere strumenti di misurazione adeguati, ha fatto sì che la maggior parte di esse si sia rivelata ampiamente non riuscita [2].

Metodologia di Assessment

Per far fronte alla sfida dell'innalzamento del livello di readiness e awareness rispetto al tema della sicurezza informatica dello strato umano di un'organizzazione, il Laboratorio Nazionale di Cybersecurity del CINI, in collaborazione con ricercatori del Centro di Ricerca in Cyber Intelligence e Information Security (CIS) dell'Università degli Studi di

Roma "La Sapienza" e del Centro di Competenza in Cybersecurity Toscano (C3T), ha dato vita al progetto *"CyberReadiness.IT"*. Il progetto, ha come obiettivo lo sviluppo di una metodologia e la realizzazione dei necessari strumenti informatici volti a valutare il livello di preparazione e sensibilità rispetto alla tematica della sicurezza informatica all'interno di una generica organizzazione.

La metodologia prevede la raccolta dati attraverso *human-based assessment*, cioè questionari utente e interviste, somministrati in loco tramite la compilazione assistita da un "tutor", ovvero in remoto tramite una piattaforma informatica (con la possibilità di analisi successiva basata su intervista diretta).

La metodologia ha come elemento cardine il legame con il *Framework Nazionale per la Cybersecurity e la Data Protection* (nel seguito *FNCSDP*)[3], al fine di allineare l'approccio a uno strumento standard, riconosciuto e ampiamente adottato per gli assessment di sicurezza informatica, permettendo il confronto tra realtà organizzative omogenee e non e differenti profili di sicurezza.

La metodologia prevede la creazione di un questionario utente dinamico, che adatti il livello di complessità delle domande sulla base delle conoscenze dimostrate dall'utente, mantenendo la capacità di comparare due o più questionari sia rispetto ai livelli di complessità attivati, sia rispetto al medesimo livello di complessità. Questi livelli derivano, dal livello meno specifico a quello più specifico, ai concetti di *Function, Category, Subcategory* e *Controlli* definiti dal FNCSDP.

Anche il legame semantico tra il framework e lo strumento di assessment vive di una duplice natura: un legame diretto mira a valutare la conoscenza e la preparazione dell'individuo rispetto ad un tema rientrante in quell'elemento (ad esempio, la corretta gestione delle password nell'ambito delle indicazioni contenute nella subcategory PR.AC-6 del framework), laddove il legame opposto mira a valutare le conseguenze di una cattiva gestione di un tema sugli elementi del framework (ad esempio, una cattiva gestione delle password ha un impatto negativo sulla protezione dei dati, come pure sulla gestione dei profili di autorizzazione).

La dinamicità della metodologia, unita al legame con uno strumento standard come il FNCSDP, abilita la possibilità di ottenere un assessment sul livello di preparazione ed awareness di un singolo impiegato dell'organizzazione, ma permette anche la sua riaggregazione verso unità operative, settori, sedi, fino all'intera organizzazione, permettendo di cogliere gli aspetti di sicurezza "scoperti" nel bagaglio culturale delle persone che ogni giorno operano con i sistemi dell'organizzazione. In aggiunta questo assessment può essere integrato facilmente in attività più strutturate di gestione del rischio cyber (e di natura più tecnologica), quali la creazione di specializzazioni del Framework rispetto a organizzazioni di interesse, settori, realtà omogenee (in gergo una "contestualizzazione del Framework") ed il relativo assessment tecnologico.

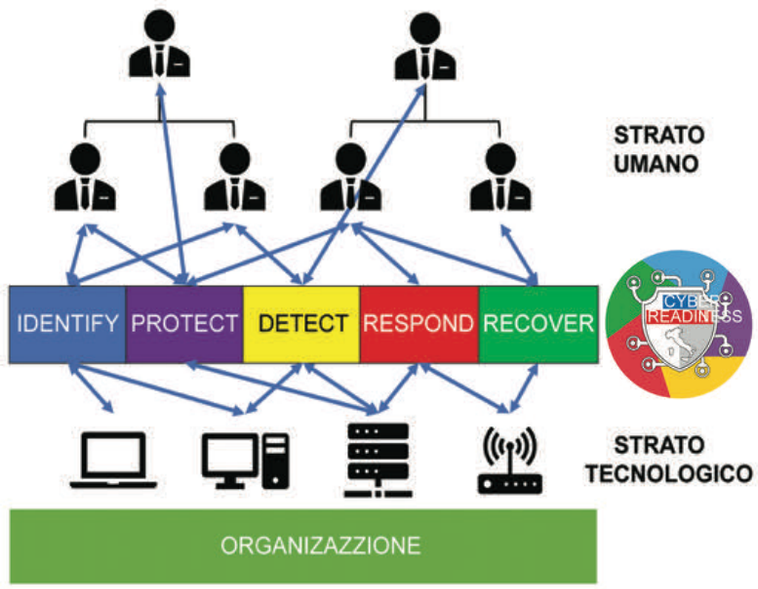
Nel caso di una grande organizzazione questa visione fornirà un utile input per valutare il rischio derivante dal comportamento dell'individuo, integrabile con i fattori di rischio che invece verranno collezionati da una procedura di assessment del livello tecnologico delle difese. Nel caso di piccole (o piccolissime organizzazioni, nel seguito PPI) dove lo strato umano è costituito da un basso numero di soggetti (spesso sotto le 10 unità), questo assessment potrà costituire una ragionevole fotografia dello stato di sicurezza informatica dell'organizzazione, avendo il vantaggio di essere meno costoso in termini di risorse e più adatto alle dimensioni e cardinalità del contesto delle PPI, o punto di partenza per ulteriori attività di assessment per organizzazioni più grandi (dalle PMI in su).

Vantaggi dell'assessment

L'applicazione della metodologia in relazione alle figure e ai soggetti coinvolti introduce numerosi vantaggi strategici, tra i quali vanno certamente annoverati i seguenti:

- La possibilità per una organizzazione di ottenere una fotografia dello stato di cyber-readiness dei suoi dipendenti, utilizzabile come base di partenza per azioni correttive (formazione/sensibilizzazione) o per integrazione come strato umano in sistemi di risk management;
- La possibilità di delineare un percorso di miglioramento individuale per i singoli individui oggetto dell'assessment, basato sulla raccomandazione di una serie di accorgimenti (quick-win) di sicurezza che mitighino inizialmente almeno le più gravi mancanze riscontrate, riducendo il rischio cyber;
- La possibilità di individuare percorsi specifici di sensibilizzazione e formazione basandosi sui risultati degli assessment, migliorandone l'efficacia;
- La possibilità di aggregare su un sistema di classificazione omogeneo i risultati provenienti dai diversi assessment, supportando attività quali la comparazione e la definizione di obiettivi da raggiungere
- La possibilità di definire prototipi di contestualizzazione (adattabili ad ampie realtà omogenee, quali settori industriali, pubblica amministrazione, PMI) basandosi sull'analisi dei dati raccolti, per catturare meglio il contesto di applicazione;
- La possibilità, per un regolatore di settore/dirigente pubblico, tramite l'analisi di questi dati in forma anonima e aggregata, di ottenere una fotografia di riferimento dello stato di cyber-readiness nel panorama italiano, utile per guidare attività di miglioramento per soggetti sia pubblici sia privati, con eventuale definizione di baseline di settore.

Infine, i risultati dell'applicazione di questa metodologia a una generica organizzazione sono integrati in un contesto più ampio di modellazione e gestione del rischio cyber basata sul FNCSDP. Questo si articola, nei passi



successivi, nella definizione di contestualizzazioni, del profilo attuale di rischio, del profilo target a cui l'organizzazione dovrebbe adeguarsi e nei sistemi di pianificazione delle attività necessarie al raggiungimento del profilo target in grado di supportare adeguatamente la prioritizzazione e il dimensionamento delle attività.

In tal senso, l'assessment di cyber-readiness aiuterà a meglio catturare le aree di interesse nel contesto più ampio di assessment di cybersecurity e a integrare quest'ultimo rispetto alle competenze/sensibilità dello "strato umano".

La metodologia descritta è attualmente in fase di test all'interno del progetto CyberReadiness.IT coinvolgendo, oltre ai soggetti promotori, una serie di partner che annoverano Torinowireless, Centro di Competenza per la sicurezza e l'Ottimizzazione delle Infrastrutture Strategiche "START 4.0" ed Anitec-Assinform: Associazione Italiana per l'Information and Communication Technology.

I risultati di questa attività, attesi per il mese di Febbraio 2020, guideranno il processo di revisione e fine-tuning, e permetteranno l'utilizzo dell'approccio su larga scala, coadiuvato dall'opportuna infrastruttura tecnologica. La presentazione de risultati è attesa in concomitanza di ITASEC20, quarta edizione della Conferenza Italiana sulla Cybersecurity.

Per maggiori informazioni è possibile riferirsi alla sito web del progetto: https://cybersecnatlab.it/cyberreadiness.

Riferimenti

[1] Rapporto Clusit sulla sicurezza ICT in Italia, 2019, https://clusit.it/rapporto-clusit/

[2] Assenza, G. et al. A Review of Methods for Evaluating Security Awareness Initiatives. European Journal for Security Research, [s. l.], p. 1, 2019. DOI 10.1007/s41125-019-00052-x.

[3] Framework Nazionale per la Cybersecurity e la Data Protection, 2019, https://www.cybersecurityframework.it ■

BIO

Il Dottore di ricerca Marco Angelini (angelini@diag.uniroma1.it) è ricercatore post-dottorato in Ingegneria Informatica presso l'Università degli Studi di Roma Sapienza, Italia, Dipartimento di Ingegneria Informatica, Automatica e Gestionale, dove ha conseguito il dottorato di ricerca nel 2017. È ricercatore presso il Center for Cyber-Intelligence and Security dell'Università Sapienza di Roma (https://www.cis.uniroma1.it), dove ha partecipato a numerosi progetti, tra cui il progetto FP-7 "PANOPTESEC", sul rilevamento automatico, la gestione e la reazione alle minacce informatiche per la protezione delle infrastrutture critiche. Marco Angelini è membro del CINI Cybersecurity National Laboratory (https://cybersecnatlab.it/), dove coordina progetti nazionali con l'obiettivo di rafforzare lo stato di sicurezza informatica di un'organizzazione, sia nel settore pubblico che in quello privato. È coautore dell'edizione 2019 del "Framework Nazionale di Cybersecurity e Data Protection" e attualmente coordina il progetto "CyberReadiness. IT" sulla valutazione dello stato di consapevolezza cyber all'interno di un'organizzazione. I suoi principali interessi di ricerca includono la Cybersecurity, sulla progettazione di soluzioni per la difesa di infrastrutture critiche da attacchi informatici, open source intelligence e analisi dei malware, e Visual Analytics, il processo di combinazione della visualizzazione dell'informazione, dell'interazione utente e del calcolo automatico per la risoluzione di problemi computazionalmente costosi, applicata al dominio della sicurezza informatica. Come risultato delle sue attività, il Dott. Ric. Marco Angelini ha pubblicato più di 40 articoli in conferenze e riviste internazionali. Maggiori informazioni su di lui sono disponibili all'indirizzo: https://sites.google.com/dis.uniroma1.it/angelini

BIO

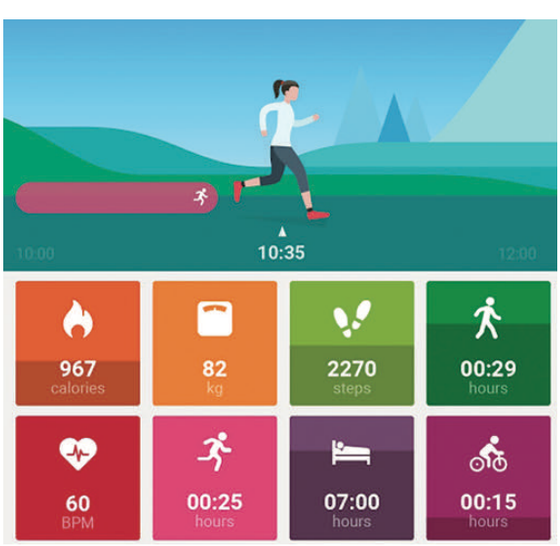
Claudio Ciccotelli (ciccotelli@diag.uniroma1.it) è un assegnista di ricerca presso il Dipartimento di Ingegneria Informatica Automatica e Gestionale Antonio Ruberti (DIAG) della Sapienza Università di Roma dove lavora all'interno del Centro di Ricerca di Cyber Intelligence and Information Security (CIS). Presso lo stesso ateneo ha conseguito la laurea magistrale in ingegneria informatica nel 2013 e il dottorato di ricerca nel 2017 con una tesi su approcci pratici per la diagnosi di guasti in data center .I suoi principali interessi di ricerca riguardano IoT e mobile security, cyber-physical security, fault detection and diagnosis in ambienti IT.

Sicurezza e privacy: una inconsapevolezza diffusa

Autore: Giancarlo Butti

La mancanza di consapevolezza circa i rischi relativi in particolare alla sicurezza o alla privacy (e alle relative conseguenze) riguarda una vasta platea di soggetti. Dai semplici utenti ai componenti dell'alta direzione delle organizzazioni, senza tuttavia escludere gli stessi esperti di sicurezza.

Il tema dei rischi relativi a sicurezza e privacy degli utenti, derivanti in particolare da comportamenti inconsapevoli di questi ultimi è stato più volte da me affrontato su questa rivista in precedenti articoli.



In particolare nell'articolo **I rischi del life-logging** evidenziavo come il semplice uso di un dispositivo indossabile dotato di GPS, utilizzato da un militare durante il suo tempo libero, avesse portato ad individuare una base militare la cui localizzazione doveva rimanere segreta. Nel caso in specie, l'aspetto più inquietante non era tanto la mancata consapevolezza del militare in merito alla sua azione (che sarebbe stata del tutto innocua nella normale vita civile), quanto il fatto che nessuna disposizione o policy fosse stata predisposta al riguardo dai suoi superiori, evidenziando la totale mancanza di un approccio security by design da parte delle forze armate coinvolte.

Questo evidenzia come l'insorgere di nuovi possibili fonti di minaccia sia una costante e come il processo di gestione del rischio sia appunto, un processo e non un evento statico e di come sia indispensabile un continuo aggiornamento delle possibili minacce che possono incombere sugli asset da proteggere.

Nell'articolo **eHEALTH: istruzioni per l'uso**, evidenziavo come l'anello debole nella catena di controllo delle informazioni sanitarie del paziente, fosse costituito per lo più dal paziente stesso.

Quest'ultimo, ad esempio, conserva sui propri dispositivi scarsamente protetti i dati sanitari in chiaro, o li inoltra utilizzando la posta elettronica, o li condivide con qualche piattaforma grazie all'uso di strumenti di misura di parametri sanitari che li archiviano sul cloud...

Rispetto alla tradizionale gestione *analogica*, basata su documenti cartacei dove l'accesso ai dati sanitari da parte di terzi potrebbe avvenire solo casualmente ad esempio durante un furto, l'accesso o la distruzione di informazioni sanitarie in formato digitale oltre che essere maggiormente

probabile, potrebbe anche costituire un'azione volontaria da parte di un'attaccante.

La mancanza di consapevolezza degli utenti provoca numerosi incidenti di sicurezza anche in ambito aziendale. Ne è una riprova la larga diffusione dei ransomware, la cui efficacia deriva in buona parte dalla facilità con cui gli utenti scaricano ed aprono documenti che dovrebbero invece insospettirli…

Nonostante le massicce campagne di informazione sul tema il costante successo di questa minaccia evidenzia come sia comunque poco percepito dagli utenti quello che debba essere il corretto comportamento da tenere in tali circostanze. Al riguardo è innegabile che la colpa va ricercata in particolare nella mancanza di policy e procedure specifiche su questo e su altri temi relativi alla sicurezza da parte delle aziende, nonostante da oltre 20 anni la normativa in ambito privacy richieda la definizione di un disciplinare e di norme di comportamento oltre che specifiche attività di formazione.

La recente estensione da parte del GDPR a tutti i Titolari dell'obbligo di notifica di una violazione di dati personali che possa comportare un danno per i diritti e le libertà delle persone fisiche, dovrebbe consentire a tutti i soggetti coinvolti di comprendere quanti e quali siano gli incidenti di sicurezza che ogni giorno coinvolgono la vita professionale (avendo al riguardo il GDPR tolto, in modo irresponsabile, qualunque vincolo e quindi qualunque tutela, in merito al trattamento di dati personali svolto nell'esercizio delle attività di carattere personale o domestico; ricordo al riguardo che viceversa, il D.Lgs 196/03 prevedeva anche per tali trattamenti l'adozione di adeguate misure di sicurezza).

Quello che si riscontra nella realtà è invece una diffusa inconsapevolezza che anche la semplice perdita di una chiavetta USB, o la rottura di un disco fisso, o la comunicazione di un dato personale alla persona sbagliata (ad esempio per il fatto che non è stato aggiornato il suo profilo di posta e continua a ricevere i messaggi destinati alla casella dell'ufficio in cui era in precedenza), costituiscono delle violazioni di dati personali.

Non è detto che da ciò derivi un obbligo di notifica. Sicuramente vi è un obbligo di annotazione nello specifico registro delle violazioni previsto dall' art. 33.5.

Un aspetto sorprendente è che molto spesso le aziende più grandi ed organizzate hanno servizi e strumenti di assistenza sia per i propri utenti interni, sia per i propri clienti, per la gestione dei malfunzionamenti dei propri sistemi e dei propri servizi.

BIO

Giancarlo Butti ha acquisito un master 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, whitepaper, 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, Università degli studi di Milano.
Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate tradizionali ed una decina on line. Ha pubblicato 21 fra libri e whitepaper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 9 opere collettive nell'ambito di ABI LAB, Oracle Community for Security, Rapporto CLUSIT…
È socio e proboviro di AIEA, socio del CLUSIT e di BCI. Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity, Rischio Informatico e GDPR di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su frodi, GDPR, eidas, sicurezza dei pagamenti, SOC, 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. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/ IEC27001, CRISC, ISM, DPO, CBCI, AMCBI.

Tali attività sono nella maggior parte dei casi tracciate, spesso con la finalità di verificare la qualità dei servizi.

Molte delle richieste di assistenza sono relative alla risoluzione di piccoli incidenti di sicurezza, ma non sono classificati come tali e quindi non vengono nemmeno annotate nell'apposito registro.

Abbiamo quindi da un lato una mancanza di analisi dei fenomeni che possono costituire un pericolo per l'organizzazione e dall'altro una violazione della normativa privacy, aggravata dal fatto che esistono le evidenze oggettive di tale violazione in quanto sia la segnalazione di anomalia, sia la sua risoluzione sono tracciati.

Anche in questo caso manca consapevolezza, mancano policy, procedure e strumenti per classificare adeguatamente cosa sia una violazione di dati personali, con grave pregiudizio sia per il Titolare (che rischia sanzioni), sia per le persone fisiche (che potranno, in caso subiscano danni, adeguatamente rivalersi sui Titolari ai sensi dell'art. 82).

Tutto questo però non stupisce: la maggior parte dei DPO, là dove presenti (per lo più per adempiere ad un mero obbligo normativo), hanno una formazione legata all'ambito legale e quindi poco consapevoli rispetto ai rischi legati alla sicurezza.

Questo è ovviamente in contrasto con i requisiti richiesti per questo ruolo, così come declinati sia dal WP29 nelle sue **Linee guida sui responsabili della protezione dei dati**, sia dal Garante europeo della privacy nel suo documento **Position paper on the role of DPO of the EU istitutions and bodies**.

Ovviamente formare adeguatamente una quantità così rilevante di soggetti su temi mai adeguatamente affrontati non è certo facile e quindi ben vengano le iniziative dell'Autorità Garante che ha attivato per i DPO sia una serie di seminari itineranti, sia una serie di webinar.

Ovviamente per quanto lodevoli, alcune ore di formazione non possono colmare queste lacune. La pubblicazione, sempre sul sito dell'Autorità Garante dell'**Handbook per i DPO** nell'ambito del progetto T4DATA colma solo in parte questa lacuna.

Infatti tale manuale (disponibile anche in italiano), tratta per lo più gli aspetti legali relativi all'attività del DPO, accenna brevemente al tema della sicurezza e si limita a citare l'attività di sorveglianza, altro grande tema largamente sottovalutato; un'anomalia questa se si considera che le attività di verifica dovrebbero costituire uno dei cardini dei compiti del DPO che, appunto, fa CONSULENZA e SORVEGLIANZA.

Per ovviare a queste lacune fortunatamente sono oggi disponibili due pubblicazioni, già citate da questa rivista:

SICUREZZA TOTALE 4.0 - L'ABC sulla physical cyber security per i DPO e le PMI (e non solo)

https://www.cybertrends.it/rivista/ numero 3/2019

Audit e GDPR - Manuale per le attività di verifica e sorveglianza del titolare e del DPO

https://www.cybertrends.it/audit-e-gdpr-manuale-per-le-attivita-di-verifica-e-sorveglianza-del-titolare-e-del-dpo/

La prima tratta espressamente del tema della sicurezza con un approccio pensato specificatamente per i neofiti e, per quanto possibile, senza l'uso di un linguaggio gergale.

La pubblicazione non è rivolta solo ai DPO, ma a quanti non avendo una specifica competenza nell'ambito della sicurezza sono chiamati, a vario titolo, a tutelare:

- i dati personali e i diritti e le libertà delle persone fisiche secondo quanto previsto dalla normativa privacy
- i beni della propria organizzazione, (gli asset aziendali, in quanto imprenditore, professionista, dirigente della PA…)
- il know how aziendale.

La seconda affronta il tema delle verifiche nell'ambito del GDPR, altra tematica questa che richiede competenze molto specifiche, che vanno ben al di là della semplice conoscenza della normativa privacy.

Essere competenti o anche esperti molto qualificati nell'ambito della sicurezza non è tuttavia sufficiente per poter affrontare una tematica complessa come il tema della tutela dei diritti e delle libertà delle persone fisiche nell'ambito della normativa privacy.

Mi è spesso capitato di trovare consulenti sicuramente molto qualificati nel loro campo, che tuttavia pensano di poter affrontare il tema dell'adeguamento alla normativa privacy come se si trattasse solo di un tema di sicurezza. Emblematico è in questo caso l'approccio all'analisi dei rischi e alle relative misure di sicurezza adottate.

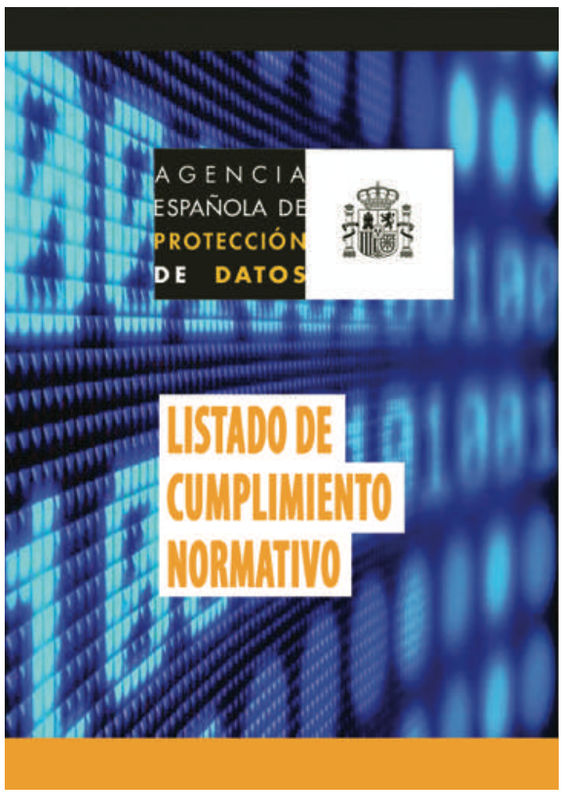
L'approccio consueto, in particolare da consulenti che operano nell'ambito delle certificazioni ISO in ambito sicurezza, è quello di riadattare qualche metodologia nota e già in uso.

Il problema di fondo è che tali metodologie sono fatte per valutare i rischi che insistono sugli asset aziendali o, nel migliore dei casi, se ci troviamo nell'ambito della ISO 27001, sulla sicurezza delle informazioni.

L'oggetto tutela dal GDPR sono invece i diritti e libertà fondamentali delle persone fisiche, un asset decisamente diverso. Inoltre, le metodologie di analisi dei rischi «classiche» prendono in considerazione i rischi dal punto di vista dell'azienda, mentre nel caso del GDPR il punto di vista da prendere in considerazione è quello delle persone fisiche che possono subire un impatto sui propri diritti.

Ecco quindi che i nostri esperti di sicurezza si trovano a produrre soluzioni assolutamente non conformi ai requisiti normativi, mettendo a rischio (sanzionatorio) i Titolari che a loro si affidano.

Tali esperti inoltre, non considerano che i diritti e le libertà fondamentali delle persone fisiche non necessariamente sono danneggiati in seguito ad una violazione di dati personali, come ben ricordano sia l'Autorità Garante Spagnola (AEPD), sia il già citato Handbook for DPO.



In particolare l'AEPD ha prodotto, nell'ambito della propria metodologia di analisi dei rischi, anche il documento LISTADO DE CUMPLIMIENTO, nel quale propone una dettagliata check list (anche se solo di impianto) in merito ai requisiti di conformità al GDPR. Non ci si può dimenticare infatti, che anche una scorretta rappresentazione su una informativa delle modalità con cui vengono trattati i dati personali, può comportare una violazione ai diritti e libertà di una persona fisica, in quanto induce l'interessato a pensare che i propri dati siano trattati in un certo modo (dando eventualmente un consenso al loro trattamento), mentre in realtà gli stessi sono trattati per altre finalità ed anche comunicati a terzi.

Che dire inoltre di quanti confondono l'analisi dei rischi con la DPIA, o che pensano che l'analisi dei rischi e le misure di sicurezza nell'ambito del GDPR riguardino gli interessati (e non le persone fisiche, come ripetutamente recita la normativa).

Il problema della consapevolezza in ambito sicurezza e privacy si pone quindi a tutti livelli e può essere superato solo con una reale volontà di formazione ed anche con una maggiore modestia da quanti si sono auto proclamati esperti in materia. ■

Awareness 2020 in Europa. Perché è già troppo tardi, tranne che per i nati della classe 2010

Fatti, esperienze, successi, fiaschi e speranze 2010-2019.

Autore: Laurent Chrzanovski

Sin dal 2010, con tutto il team della Swiss Webacademy, ma anche a titolo individuale dell'autore, abbiamo sviluppato e sviluppiamo tutt'ora numerose attività di *awareness* in diversi paesi ed ecosistemi dell'Unione Europea - tra le quali anche la rivista che state leggendo.

Al di fuori del mondo delle scuole medie - sul quale torneremo e nell'ambito del quale possiamo ancora intravedere progetti promettenti - ci guardiamo bene ormai dal parlare di *"soluzioni di successo"* vista l'accelerazione delle tecnologie – e vorremmo approfittare di questo spazio per condividere la più oggettiva delle osservazione possibili su quanto è successo durante gli ultimi anni di questa decade in questo campo.

Dal 2010 al 2016: un'epoca di "gloria" revoluta

"Storicamente" parlando, dato il frenetico ritmo del digitale, sino alla metà di questo decennio, corsi brevi e accattivanti di awareness di base erano non solo voluti ma persino plebiscitari, dalle scuole ai semplici cittadini, dalle piccole imprese ai giganti dell'industria e del settore terziario.

Il pubblico rispondeva presente. La nostra realtà richiedeva soltanto piccoli aiuti, in termini logistici – *ad es. oggettistica "gadget" per i concorsi per i bambini* – che di minimi rimborsi che permettevano al nostro team di non lavorare in perdita.

Furono proprio quegli *"anni di gloria"* che ci hanno permesso, su richiesta delle Nazioni Unite, di lanciare la rivista trimestrale *"Cybersecurity Trends"*, raggiungendo rapidamente 4 versioni differenti in altrettante lingue.

L'*"ondata"* favorevole della diffusione di un'awareness di qualità, per il mondo dei minori e di chi ne ha la tutela, ci ha permesso di tradurre e pubblicare in lingua rumena e in lingua italiana i manuali per bimbi e per genitori dell'Unione Internazionale delle Telecomunicazioni (ITU).

In particolare, con il costante sostegno dell'ITU, siamo riusciti ad ideare, a tradurre e poi a portare in ben 5 paesi, inclusa l'Italia, la mostra didattica *"Eroi e vittime dei social media. Dai geroglifici a Facebook"*.

In Italia, grazie al costante appoggio e sostegno di Poste Italiane e della Fondazione Global Cyber Security Center, i manuali ITU e la mostra sono stati letti/visitati da centinaia di migliaia di cittadini. La stessa mostra continua ad essere veicolata da Poste Italiane sia nelle scuole che in molti eventi di spessore culminati con il MakerFaire di Roma (200'000 visitatori, ottobre

2017), dove fu esposta in un bellissimo spazio curato da Poste Italiane e condiviso con la Polizia Postale e delle Comunicazioni.

Proprio in quella mostra, anticipammo quello che stava già accadendo: uno slittamento sempre più rapido della tipologia di *"attacchi"* e dell'esposizione del singolo individuo qualsiasi fosse la sua età e il suo stato socio-professionale: il mondo dei data/dell'informazione e della loro manipolazione stava già diventando il punto centrale del problema.

Il clash informazionale del 2016 e le sue conseguenze sull'awareness

Fino al 2016 le attività didattiche della Swiss Accademy erano destinate, in equa parte, ad insegnare tecniche operative di base ed a capire cosa e come postare o scaricare nel net.

Una prima categoria comprendeva la prevenzione contro gli errori di configurazione – *tipicamente insegnare l'attualizzazione dei programmi e dei sistemi per garantire il buon funzionamento degli antivirus* –, l'attivazione di misure tecniche di base per garantire la propria privacy nell'uso del laptop o del cellulare – *come la disattivazione del GPS quando non necessario, la diffidenza dei wifi pubblici o senza password* – e, infine, l'individuazione dello spam, dello scam e dei segnali di manomissione a distanza dei propri sistemi IT&C (generalmente "semplici" virus malevoli) per riportarli al più presto a specialisti e/o alle forze dell'ordine.

Nella seconda categoria, si insegnava un decalogo di *"best practice"* su cosa postare, chi accettare e chi rifiutare sui social network, sottolineare l'intrusività di un certo numero di siti e ribadire che la gratuità non è un assioma del net, anzi, che ad ogni *"I accept"* di contratti di usufrutto di software gratuiti vi sono conseguenze e che il click di principio equivale alla propria firma autografa su di un contratto cartaceo – un aspetto questo ancora incompreso in Europa.

Vi era quindi una *"comunità"* uniforme, dai bimbi agli adulti, che doveva e voleva essere informata delle varie configurazioni e regole di sicurezza base per poter usufruire serenamente delle infinite possibilità che il mondo digitale offriva.

Dalla fine del 2016, con l'avvento della 4G, l'equazione di base è cambiata completamente. Alimentato da migliaia di informazioni ogni giorno *"sfogliate"* ad alta velocità sul piccolo schermo del proprio smartphone, l'individuo del 2020 è talmente immerso nel digitale che persino la sua sicurezza fisica non costituisce niente di più che una parte minoritaria della propria sicurezza del suo ecosistema in *extenso*.

Ed è così che tutto quello che costituiva l'awareness *"pre-4G"* non rappresenta più che una cortissima introduzione, in un mondo dove la vera minaccia per gli individui non è più una mancanza di educazione di base meramente legata all'uso delle tecnologie, bensì ad una totale assenza di cultura generale nell'uso e abuso del proprio smartphone.

Sul piccolo schermo, si accede ormai a tutte le attività quotidiane: notizie, giochi e la costante comunicazione con terzi. Si mischia allegramente vita pubblica, professionale e privata e si cerca o si immettono on line informazioni strettamente riservate, sia intime che professionali.

Awareness 2020: (im)possibile entrare nei preconcetti dei cittadini?

L'awareness *"post 5G"*, per essere utile, deve quindi riflettere questo cambiamento radicale di paradosso, slittando dalla tecnologia in senso stretto al contenuto consultato.

BIO

Dottore di ricerca in Archeologia romana dell'Università di Losanna, Laurent ha poi ottenuto un diploma post-dottorale in Storia e Sociologia presso l'Accademia delle Scienze della Romania, l'abilitazione UE a dirigere Dottorati di ricerca nel campi della Storia e delle scienze affini. Oggi, Laurent è professore presso la Scuola dottorale e postdottorale dell'Universita' Statale di Sibiu. Tiene regolarmente corsi post-dottorato in Università di prestigio in diversi paesi dell'UE, in primis a Varsavia. E' autore/redattore di 31 libri, di oltre un centinaio di articoli scientifici e di altrettanti articoli destinati al grande pubblico.
Nel campo della cybersecurity, Laurent è membro e consulente contrattuale del gruppo di esperti dell'ITU. Ha fondato e gestisce ogni anno il trittico di congressi PPP "Cybersecurity Dialogues" (Romania, Svizzera, Italia) organizzati in collaborazione con un grande numero di istituzioni specializzate, internazionali e nazionali. Nello stesso spirito e con lo stesso spirito e con i stessi partner, è fondatore e redattore capo e redattore capo di Cybersecurity Trends, la prima rivista trimestrale di sensibilizzazione alla sicurezza informatica per adulti, pubblicata in quattro varianti adattate ad altrettanti ecosistemi lingusitsici e culturali. Il suo campo di studio è focalizzato sulla relazione tra i comportamenti umani nel mondo digitale e il bisogno di trovare il giusto equilibrio tra la sicurezza e la privacy per l'utente finale, cioè "l'e-cittadino" che siamo tutti diventati.

E' doveroso ricordare che proprio quest'anno si è rilevata una morte quasi sicura dei *tablet* a causa di un definitivo stravolgimento della tecnica d'accesso al flusso dell'informazione sia questa generale che riservata: le informazioni infatti sono ormai consultate per il 72% via smartphone, per 25% via il laptop e solo per il 3% via *tablet*.

Un fatto almeno altrettanto importante è il numero oramai superiore di uploads rispetto ai download - iperconnessione delle persone *(anche se lo smartphone è in standby)*, moltiplicazione automatica dei dati nei social network e nelle news feed, *(spesso attività più algoritmica senza l'intervento umano)* e la crescita smisurata degli oggetti connessi.

Diventa quindi obbligatorio entrare proprio in ciò che troppi adulti non vogliono condividere né discutere: le basi culturali, etiche, morali e storiche che permettono di creare un'igiene di vita digitale, il solo mezzo per ridurre drasticamente la superficie d'attacco di ogni singolo cittadino e, conseguentemente, della sua famiglia, dei suoi cari e dell'azienda dove lavora.

Parlare di *"rinuncia"* alla libertà di poter scaricare tutto - atto per altro delle volte illegale – o di evitare o limitare l'uso di certe App o social network, di usare due smartphone per dissociare quanto possibile la vita personale da quella professionale appare, per molti, una vera e propria intrusione nella vita privata.

Quante volte abbiamo sentito, da adulti, la frase *"so cosa faccio!"*. Il vero e proprio sovraccarico di informazione, spesso approssimativa, manomessa o addirittura contraffatta, fa così credere ai molti, che presuntuosamente pensano di sapere già quello che devono o devono non fare sulla rete specialmente col piccolo smartphone, che i rischi sono pochi.

Assistiamo quindi ad un calo di interesse per l'awareness, specialmente nel mondo degli adulti. Questa credenza nell'onnisapienza (*"wikipediana"* come la definiscono gli esperti) porta notevoli danni. Quando, in ambito professionale, spieghiamo l'intrusività delle majors e dello spionaggio economico proprio grazie ai dati offerti online dalle vittime inconsapevoli, la risposte che ci vengono fornite sono spesso: *"sono troppo piccolo per interessare chiunque"* o, cosa peggiore per le aziende, *"ho acquistato le soluzioni idonee ed ho un capo sicurezza"*…

Ho i tuoi filmati porno e anche la tua password: nessuna presa di coscienza dopo gli scam

Per offrire un chiaro esempio, negli ultimi due anni non vi è stata nessuna presa di coscienza collettiva a fronte delle numerose denunce presentate alle forze dell'ordine di tutta l'Unione Europea, a seguito dello tsunami di spam minaccioso e dal contenuto personalizzato e intimissimo, aggravato per giunta dal fatto che lo stesso forniva come prova il possesso della password della mail personale della vittima.

Non ha suscitato nessuna riflessione sull'intrusione del mondo digitale il fatto che numerose bande criminali hanno ricattato milioni di vittime minacciando, di volta in volta, di divulgare a tutti i contatti della vittima, le registrazioni compromettenti acquisite tramite webcam del loro laptop quando ,a loro detta, avevano visitato siti pornografici.

L'allerta, dovutamente trattata dai CERT e dalle Polizie di Stato dell'UE, è stata rapidamente spiegata come una estorsione da parte di cybercriminali basata su filmati inesistenti e che colpiva centinaia di milioni di indirizzi email e password compromessi nel 2015-2016.

Passata la prima suggestione, in un modo quasi bipolare, questo fenomeno è stato quasi ignorato dai grandi media e al posto di suscitare una riflessione sul nostro modo di vivere nel mondo digitale si è trovato il pretesto che, chi ha pagato non si è dovutamente informato e che le «prove» in possesso dei ricattatori non sono mai esistite. In parallelo, i crypto-ransomware continuano ad esistere e a fare stragi di piccole e medie imprese, ma non fanno più *"breaking news"* da molti mesi perché non si mietono più vittime di alto profilo come fu all'inizio per le infrastrutture critiche e gli ospedali.

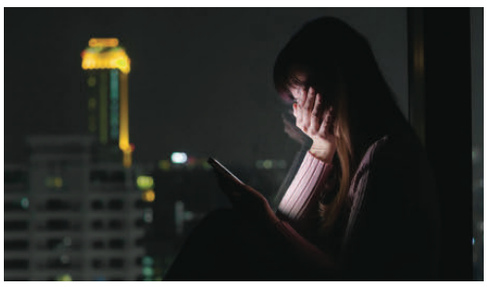
Questa *"censura"* mediatica degli eventi considerati *"piccoli"* ha delle ripercussioni molto gravi. In effetti, troppo spesso durante nostre attività di awareness, alcuni rari imprenditori, dopo il corso e solo a tu per tu, confessano di essere state vittime chiedendo consigli ma nessuno di loro finora ci ha mai testimoniato di aver sporto denuncia alle autorità competenti, al contrario molti hanno pagato i riscatti ai criminali.

Al posto di diventare un atto banale - come denunciare del furto di un autoveicolo – l'essere vittima di un reato digitale sta generando omertà e, come spiegano molti psichiatri con la sindrome "della donna da trauma dello stupro", genera una percezione sbagliata di colpevolezza attitudinale che avrebbe permesso di essere preda dei criminali e che rappresenta un evento che non si vuole raccontare a nessuno.

Campagne di awareness vere ma ignorate, campagne fake invece con grandi consensi: non solo il cyber è vittima

Proprio a causa del *"caos dell'informazione"*, titolo del libro di Antonio Martusciello, sul quale torneremo in conclusione, che genera il "so cosa faccio", l'awareness, e non solo quella rivolta al digitale, ha perso molto del suo coinvolgimento verso il grande pubblico.

Persino le campagne contro le reali epidemie di salute pubblica non fanno più notizia. L'esempio odierno più evidente è quello dell'allarme dato



da medici e dai Ministeri della Salute di tutta l'UE. Trattasi della crescita esponenziale delle malattie sessualmente trasmissibili.

Nonostante la gravità di tali malattie, massicciamente riapparse da quando, passata la paura dell'AIDS – *malattia ormai confinata e contrastata da medicine efficaci* – assistiamo alla rinnovata moltiplicazione di incontri occasionali non protetti e non vi sono né soldi, né volontà di fare opere di prevenzione *urbi et orbi* a riguardo.

All'opposto, vengono compiute vere campagne di fake awareness, come quelle anti-vaccini , in particolar modo quelli obbligatori per bambini, sapientemente gestite online da vari gruppi sociali e religiosi e che sono sempre più difficili da contrastare da parte delle autorità competenti.

In questo quadro, l'awareness digitale, molto più complesso rispetto quello svolto su altre tematiche di sicurezza, appare poco compreso, negletto e quindi tralasciato da troppi governi che si susseguono in quasi tutti i paesi dell'UE.

Proprio per la multiforme dimensione dei pericoli – da quelli tecnici, tecnologici fino a quelli informazionali – nel 2020 una awareness completa non potrà ambire ad una chance di successo collettivo se non sarà promossa proprio dai maggiori enti statali – non più dalle solite ONG che, anno dopo anno, ricevono meno risorse per condurre a buon porto la loro missione.

Dopo un trentennio di voluto ostruzionismo politico, le poche ONG presenti sul territorio si ritrovano, con l'aiuto benevolo delle forze dell'ordine, a dover fare una indispensabile *awareness* di base al posto degli Stati o degli enti statali, *in primis* i Ministeri dell'istruzione nazionali, dicasteri che a loro volta non hanno avuto il diritto di fare nessuna attività tramite le strutture loro subordinate come scuole, università, enti di formazione professionale.

Per trent'anni, quasi tutti gli stati europei ad eccezione della Finlandia - e parzialmente della Gran Bretagna - hanno messo a disposizione di professori, bimbi e - raramente - adulti… siti web e materiale scaricabile.

Questo espediente, e cioè l'affidamento di manuali pdf a professori di altre materie che avrebbero dovuto leggerli, capirli e poi insegnarne la sostanza, provato in quasi tutti i paesi dell'UE via *Safernet*, ha dato risultati a dir poco inesistenti. E' necessario ricordare in questa sede che l'obbligo europeo di tradurre e promuovere i manuali di Safer Internet è, nella maggioranza dei paesi membri dell'UE, affidato a *"charity business NGOs"*, un vero e proprio business che spesso impiega sino al 80% delle risorse ricevute, per pagare stipendi, sedi, bisogni di funzionamento quotidiano nonché costose campagne pubblicitarie, destinando solo il 20% al progetto ed alla sua implementazione quindi dando resultati insoddisfacenti e giustificando le critiche governative su quanto realizzato a fronte di quanto speso.

Ex Scandinavia lux: ma ne abbiamo ancora il coraggio?

Come abbiamo scritto, solo la Finlandia ha introdotto in tutto il cursus scolastico una formazione continua sulla sicurezza digitale. Dal 2014 ha saputo istituire: corsi obbligatori a tutti i livelli e, nelle scuole, ha inserito l'apprendimento circa le *"fake news"* integrandola in ogni disciplina e non come tematica a se stante, come magari lo è la sicurezza digitale di base.

Vista la sua popolazione (5.5 milioni di abitanti, immigrazione molto limitata), il piccolo paese scandinavo non deve certo affrontare seri problemi di sensibilità sociale e multiculturale che a differenza hanno i grandi paesi dell'Europa occidentale. Riesce quindi ad favorire efficacemente, con esempi di palesi *"fake news"*, lezioni introduttive presenti tutt'oggi in moltissimi paesi dell'UE, su temi quali l'educazione civica, l'educazione religiosa e - sempre di meno - quella sessuale.

In quest'ultimo campo, quello dell'educazione sessuale, la Finlandia è riuscita, tramite esempi digitali, a far diventare attuale una materia altrove obsoleta, una obsolescenza dovuta da una mancata corrispondenza tra i contenuti pornografici presentati e quelli visti dagli stessi alunni o magari dovuti ad eccessi dell' ondata della *"gender equality"*, fenomeno che sta pian piano imponendosi anche in Europa.

E' doveroso parlare anche del ruolo vitale l'approccio finlandese ha nel salvaguardare il contenuto dei manuali ufficiali di storia o di biologia, ancora efficaci in alcuni paesi come l'Italia, quotidianamente messi in crisi dalle

numerose *"false storie"* e dai movimenti anti-darwinisti che, sulla carta, ottengono molto più successo.

Ciò facendo, la Finlandia ha aperto una strada che, da poco, anche India e Russia hanno adottato. Ha proibito

l'introduzione dei telefonini nelle scuole, additandolo come un punto dolente per molti Stati e cittadini europei.

Vietare gli smartphone durante le lezioni è infatti l'esempio più tangibile che l'essere sicuri vuol ANCHE dire rinunciare - o posticipare - un certo numero di "libertà" tra i mille privilegi che ci siamo concessi nel mondo digitale, talvolta immorali o poco legittimi e in assenza di leggi e regolamenti.

Le basi del programma legislativo, educativo e trans-ministeriale finlandese, che oggi porta i suoi frutti al di là delle migliori speranze, sono nate proprio nel 2014 anno in cui il governo di Helsinki, molto sensibile alla sovranità nazionale, ha intrapreso questa iniziativa – come fecero anche altri paesi come India, Russia e ovviamente Cina. Tali nazioni hanno saputo ascoltare le commissioni di ricerca e non, al contrario, le promesse di facili introiti, rimettendo in primo piano la sicurezza strategica nazionale e quella di propri cittadini (non entreremo in questa sede nei criteri politici).

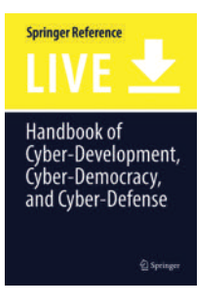
Sempre nel 2014, a distanza di un mese, fu reso pubblico il rapporto del National President of Security Telecommunications Advisory Committee *(NSTAC Report to the President on the Internet of Things)* e iniziava con questa frase: *"There is a small – and rapidly closing – window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations".* Il Report dell'UK Government office for Science *(The Internet of Things: making the most of the Second Digital Revolution)*, con prefazione dell'allora Premier David Cameron, invece non vedeva che benefici da trarre dalle nuove tecnologie… inutile dire in Europa, quale dei due pensieri fu plebiscitario…

La Finlandia seppe leggere bene i vari rapporti tra moltiplicazione degli oggetti IoT e le moltiplicazioni esponenziali di generatori e ripetitori di informazioni, specialmente quelle che avevano particolare successo come le opere di ed azionò già in modo preventivo. Gli altri stati dell'UE hanno preferito, visibilmente, le promesse progressiste del rapporto inglese e di molti altri dal contenuto analogo.

Europa, 2020… chi e come può agire: l'Italia in posizione vantaggiosa

Tornando all'awareness europeo, dopo un trentennio di abbandono quasi totale, la situazione odierna appare gravissima: abbiamo dimostrato in innumerevoli occasioni che non si tratta di un tema banale che deve essere necessariamente *"insegnato"* di persona – non tramite materiali scaricabili – e che non può essere incluso in strategie che non vedano l'implicazione massiccia e diretta del Ministero dell'Istruzione nazionale in collaborazione con gli Enti specializzati nella sicurezza strettamente tecnica e quella delle informazioni.

Purtroppo, questa opzione non sembra essere presente sul tavolo di molti governi, anche per il banale motivo che implicherebbe l'assunzione



di professori addizionali e la costituzione di speciali commissioni interministeriali alle quale incomberebbe l'arduo compito di aggiornare almeno mensilmente le varie problematiche, seguendo l'esempio del *"handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense"* opera del gruppo di ricerca dell'editore Springer.

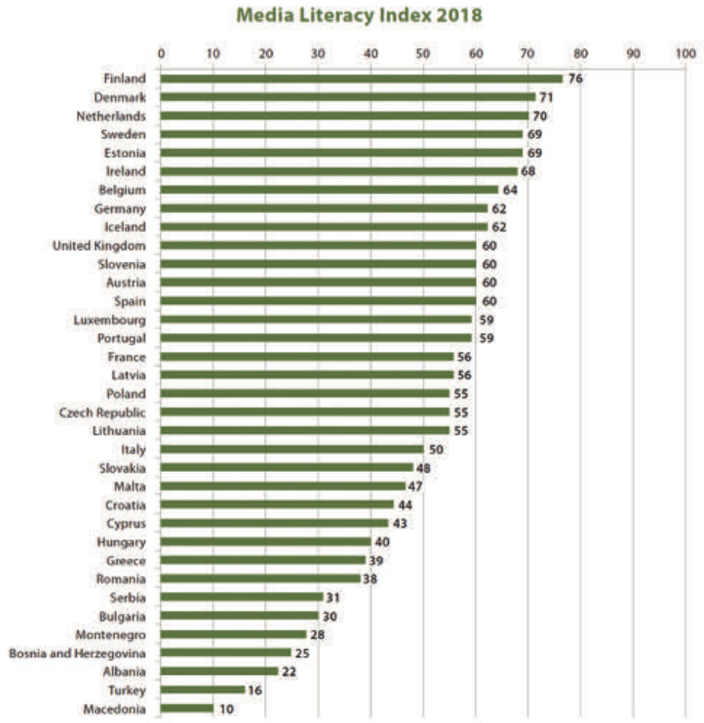
Il lato positivo della medaglia è che proprio le ONG e i grandi gruppi (come la Fondazione GCSEC di Poste Italiane) potrebbero contribuire in una piccola ma cospicua parte a questo lavoro di *"reazione immediata"*. Certo è che le stesse da sole, non potranno mai assicurare la capillarità sull'intero territorio e la costanza dell'insegnamento che questo tema realmente necessita.

Da sottolineare in questo ambito, che un'iniziativa di stampo finlandese non sarebbe possibile oggi nel Bel Paese data l'assenza di decenni di riforme e controriforme dei manuali scolastici (basta menzionare a questo effetto le perenni riforme dell'insegnamento di grammatica e ortografia in Francia, che hanno portato ad un vero disastro, con nostri dottorandi incapaci di scrivere un solo paragrafo correttamente, o dei manuali di storia *"politically correct"* del mondo anglosassone, e non solo, dove molti episodi - come le crociate o la colonizzazione - sono ormai totalmente censurati o resi con sfumature che sfiorano la disinformazione).

Peraltro, nella tabella europea nell'ultimo rapporto sulla capacità culturale di leggere una notizia e classificarla come palesemente falsa, semi-falsa o veritiera *"media litteracy index"*, l'Italia, con 50 punti, si trova in una posizione "salvabile".

Peraltro, date le frequenti attività in molte città europee portate avanti da chi scrive, possiamo affermare che, per quanto riguarda l'interesse delle case editrici e dei lettori per i pericoli del mondo digitale, se le grandi librerie di UK o Russia propongono più di 5'000 titoli all'anno, il lettore della lingua di Dante non è tra i più trascurati in Europa, anzi.

In Italia, appaiono annualmente almeno 500 nuove monografie, da mettere in paragone con meno di un centinaio per Francia o Germania e con appena una dozzina negli altre realtà i europee. Anche qui, c'è possibilità di gettare le fondamenta di una *awareness* ben ideata e destinata agli adulti,



Tratto dal Rapporto 2018 dell'Open Society Institute, scaricabile online a: http://osi.bg/downloads/File/2018/MediaLiteracyIndex2018_publishENG.pdf

ma anche qui, è necessario che ci sia una presenza ed un sostegno dei vertici più alti a livello governativo.

Infine, l'assenza fino a pochi giorni fa di un CERT Unico Nazionale dotato di sufficienti mezzi e uomini ha – *e non è un controsenso* – giovato al paese poiché possiamo affermare che il numero di CERT di settore in Italia, di università con curricula aggiornati, "all'americana", di Centri di Sicurezza pubblico-privato, regionali o professionali, rappresenta una dato positivo di specificità italiana che non trova riscontri in paragone col resto dell'Europa come nei paesi ultra-centralizzati.

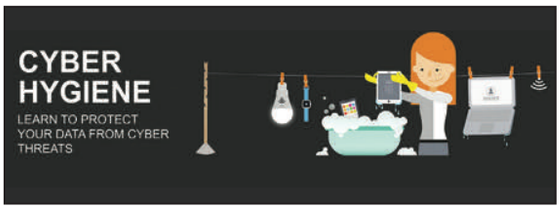
L'unico metodo possibile: fornire a tutti basi culturali e spiegazioni di una Digital Hygene, lasciando ad ognuno libero arbitrio.

Come abbiamo visto, in tutta Europa, la oramai trentenne carenza di lungimiranza di governi consecutivi, i disaccordi tra dirigenti dei vari ministeri competenti (telecomunicazioni, interni, educazione) e enti subordinati hanno contribuito a creare l'inimmaginabile.

Mentre esiste ancora una censura di Stato con Enti e normative adeguate per media, mezzi audiovisivi e stampa, per Internet invece, e non solo a causa della sua dimensione globale e della sua intrinseca extraterritorialità, sembra essere rimasto tutto (o quasi) senza controllo.

Ancora peggio, stiamo assistendo e subendo una nuova censura da parte dei giganti dei Social che non ha una base etica, morala, ideologia o religiosa, …

L'*awareness* del 2020, anche grazie ai dati che avremo modo di leggere nelle recensioni dei capolavori di Shoshanna Zhuboff e di Michel Onfray, dovrà quindi essere un'azione profondamente educazionale e culturale ed essenzialmente supportata e appoggiata da Enti statali, con lo scopo primario di mettere ogni alunno ed ogni adulto di fronte alle molteplici scelte di vita, soprattutto morali, spiegandone i pro ed i contro.



Ma in primis ognuno di noi dovrà rispondere a due fondamentali domande. La prima: *come cittadino, ho ancora fiducia nelle Istituzioni della Nazione?*

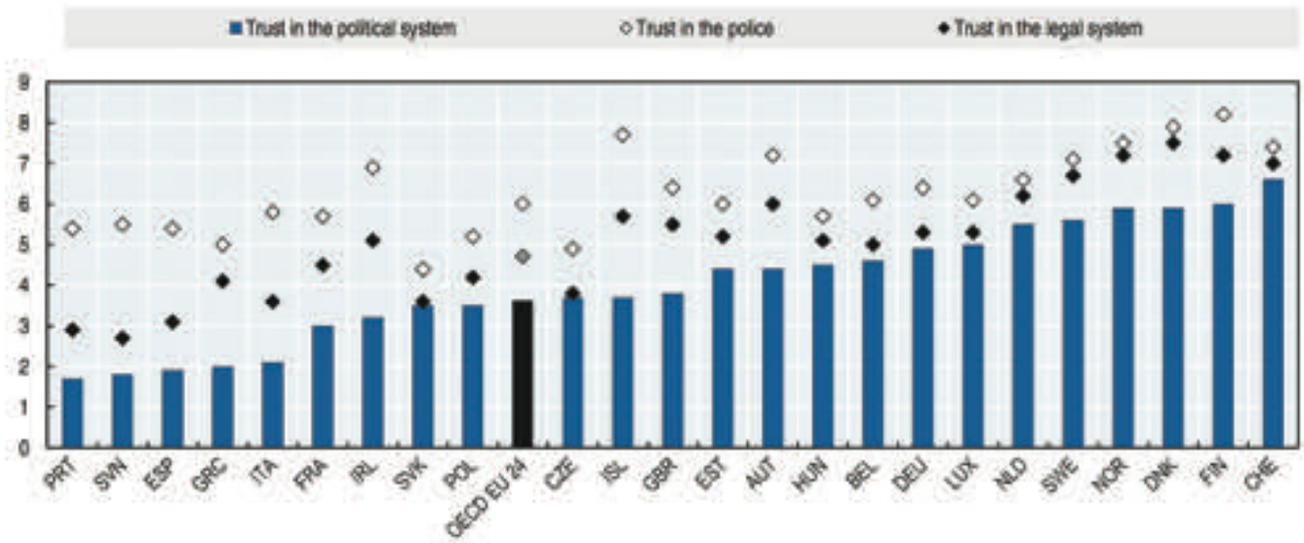
E se sì, *a che libertà digitale sarei disposto a rinunciare a beneficio della sicurezza fisica, digitale ma anche informativa, pubblica, privata e intima propria e dei suoi cari?*

Appare ormai chiaro che se, a queste due domande, la risposta è negativa, a causa della confusione tra fiducia nel mondo politico e fiducia nelle istituzioni statali, ognuno sarà solo ed esclusivamente responsabile del suo destino. E qui, purtroppo, l'Italia è nei 5 paesi europei nettamente in coda per quanto riguarda la fiducia accordata non solo al sistema politico ma pure a quello legale e giuridico. Per ora, solo le forze dell'ordine beneficiano ancora della fiducia di una maggioranza di cittadini.

Se invece, in corrispondenza del rispetto portato alle forze dell'ordine, la risposta è positiva, appare improrogabile l'impegno dello Stato nel mettere in campo con tutte le sue forze tutte le azioni volte a educare e bloccare contenuti palesemente illegali, e a far sì che ogni iniziativa di awareness proponga ai cittadini la soluzione concreta e giuridicamente condivisa dal Commissario dell'Autorità Garante delle Comunicazioni. *(Martusciello, Antonio; Petti Rosaria, Il caos dell'informazione, Società Dante Alighieri, Milano 2019).*

Senza attendere l'intervento di Bruxelles, lo Stato, con l'aiuto del settore privato , può iniziare a proporre ai propri studenti e cittadini una classificazione di attendibilità per tutte le informazioni (dal fatto e le sue interpretazioni argomentate alle sue contraffazioni). Si eviterà così di ricorrere in futuro ad una censura reiterata e renderà molto più facile il lavoro per tutte le iniziative di *awareness* in tema.

Rimarrebbero allora vittime della propria incoscienza e delle proprie azioni digitali solo coloro che non si doteranno delle precauzioni minime e desidereranno credere in dati palesemente falsificati o fabbricati, una rara eccezione se si pensa all'intera popolazione del mondo d'oggi.



Note: Response options range from 0 ("No trust at all") to 10 ("Complete trust"). The OECD EU average is the population-weighted average of the values included in the chart.

Source: Eurostat (2015), European Union Statistics on Income and Living Conditions (EU-SILC), http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=ilc_pw03&lang=en.

Per concludere, l'awareness del 2020, non avendo basi responsabili dalle quali crescere, dovrà sorgere come un elemento odierno in ogni momento della vita formativa dell'individuo parallelamente allo sviluppo frenetico delle realtà informative e tecnologiche. La sua costituzione sarà *in primis* culturale ed educativa, per sradicare in ogni campo preconcetti e idee sbagliate e soltanto poi dovrà dimostrare i pro ed i contro dell'uso di ogni singola tecnologia, app o sito.

Solo demistificando il falso, come fatto in Finlandia, si potrà ritrovare una cultura di base sana e solida. Senza di essa, nessuna awareness può protendere al successo, perché verrà subito considerato come l'apologia della privazione della libertà di espressione e come un'intrusione nelle scelte personali dell'uso del web e degli strumenti che ne permettono l'accesso. ■

Ricevi gratuitamente la newsletter registrandoti sul nostro sito:
www.gcsec.org/newsletter-1

Convergenza e complementarità tra perimetro di sicurezza nazionale cibernetica edirettiva NIS

Autore: Gianluca Bocci

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.

Sono passati appena 6 mesi dalla pubblicazione dell'ultimo articolo in materia di sicurezza cibernetica con il quale illustravo gli aspetti principali inerenti al nuovo Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio, il c.d. *"Cybersecurity Act"*[1]. Recenti interventi legislativi ci portano ancora una volta ad approfondire come l'ecosistema di sicurezza cibernetica del nostro Paese sta evolvendo.Lo scorso 21 Settembre veniva infatti pubblicato in G.U., il d.l.n°105, recante *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"*, l'8 Novembre, il DPCM recante *"Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano"* e infine il 20 Novembre 2019[2], la Legge del n°133/09 del 18 Novembre, recante *"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*[3]*"*. Con quest'ultimo provvedimento è stato convertito, con relative modificazioni apportate dalla Camera dei Deputati e dal Senato della Repubblica, il già citato d.l. n°105.Si tratta di provvedimenti di grande interesse e rilevanza per il nostro Paese, capaci di stimolare nelle loro complesso riflessioni e considerazioni sull'evoluzione del nostro ecosistema di sicurezza cibernetica, a partire dal perimetro di sicurezza nazionale cibernetica, nonché dal rapporto che vi intercorre con la c.d. direttiva NIS e la sua attuazione nazionale, grazie al d.lgs. n° 65 del 18 Maggio 2018.

Perimetro di sicurezza nazionale cibernetica

Con la conversione in legge del d.l. n°105 del 21 Settembre 2019, viene costituito il perimetro di sicurezza nazionale cibernetica e contestualmente disciplinati i poteri speciali del Governo nei settori di rilevanza strategica. Prima di entrare nel merito dei principali elementi che caratterizzano il perimetro di sicurezza nazionale cibernetica, si desidera ricordare, se pur sinteticamente, come è nata e poi si è evoluta in questi ultimi anni, l'architettura di cyber security che è di riferimento nel nostro paese, sulla quale poggia proprio il perimetrononché la direttiva NIS.

Con il DPCM del 24 gennaio 2013, il c.d. Decreto Monti, veniva costituita l'architettura designata per la tutela della sicurezza nazionale delle infrastrutture critiche materiali e immateriali, con particolare riferimento alla protezione cibernetica, specificandoe attribuendo i compiti di ciascuna componente individuata, nonché le procedure utili per limitare le vulnerabilità, prevenire i rischi, rispondere tempestivamente agli attacchi e ripristinare in maniera il più celere possibile le funzionalità dei sistemi impattati. In attuazione al DPCM seguiva la pubblicazione del *"Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico"* e del *"Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica"*, che tracciavano gli obiettivi che il Governo si era prefissato, e come già in parte accennato, attribuivano contestualmente ruoli e responsabilità a tutte le parti coinvolte affinché potessero garantire in maniera coordinata un efficace ed efficiente capacitàdi protezione cibernetica.Con il DPCM del 17 Febbraio 2017, il c.d. decreto Gentiloni, e alla luce della Direttiva NIS, veniva rivisitata l'architettura, soprattutto in termini di ruoli e responsabilità, che trovava nel comparto dell'intelligence, con il Dipartimento delle informazioni per la sicurezza (DIS), il nuovo baricentro del governo dei processi funzionali alla protezione cibernetica.Traendo vantaggio da questa complessa macchina organizzativa, già disponibile ed orientata ai temi della cyber security, hanno trovato terreno fertile per essere accolte:

- la Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, già precedentemente indicata come direttiva NIS che, recepita in Italia con il d.lgs. n° 65 del 18 Maggio 2018 che si pone l'obiettivo, a livello comunitario, d'innalzare la sicurezza cibernetica di tutti quei soggetti che forniscono e in tal senso possono garantire l'erogazione di quei servizi essenziali per il mantenimento di attività sociali e/o economiche da cui dipendono i cittadini, le imprese e i mercati in generale. Proprio in questo frangente, con un adeguamento dell'architettura nazionale di cyber security, viene costituito il CSIRT Italiano[4], presso la Presidenza del Consiglio dei Ministri, con lo scopo primario di gestire le notifiche di incidenti informatici da parte degli operatori di servizi essenziali, attività precedentemente svolta dal CERT Nazionale[5] per le imprese e cittadini e dal CERT-PA[6] per i soggetti appartenenti alla Pubblica Amministrazione. Gli aspetti organizzativi del CSIRT Italiano trovano disciplina proprio nel recente DPCM pubblicato l'8 Novembre 2019, recante *"Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano"*.
- il d.l. n° 105 del 21 Settembre 2019 che, convertito in Legge il 14 Novembre 2019, definisce il *"Perimetro Nazionale di Sicurezza Cibernetica"*, che a differenza di quanto indicato nel precedente puntopone invece l'attenzione e ha l'obiettivo di assicurare un elevato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici di soggetti da cui dipende l'esercizio di una funzione essenziale dello Stato e con i servizi erogati possono pregiudicare la sicurezza nazionale.

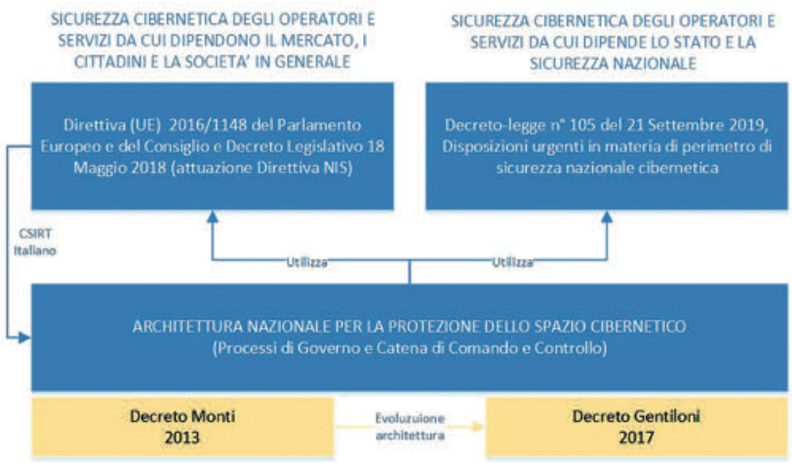


***Figura1** - Ecosistema "olistico" per la protezione dello spazio cibernetico del Sistema-Paese*[7]

Sono dunque sostanzialmente diversi gli obiettivi che s'intendono perseguire con il Perimetro di Sicurezza Nazionale Cibernetica e la Direttiva NIS. Se da un lato la Direttiva NIS si concentra su tutti quegli elementi essenziali per i quali risulta evidente il ruolo centrico verso una *"sicurezza dei mercati*[8]*"*, per il Perimetro di Sicurezza Nazionale Cibernetica risulta centrico verso la *"Sicurezza dello Stato*[9]*"*, ragion per cui in quest'ultimo caso sono chiari ed inequivocabili anche i riferimenti alla protezione delle reti 5G e all'ampliamento della Golden Power come la relativa estensione dei poteri speciali del Governo sui settori tecnologicamente avanzati.

Per queste ragioni, il Perimetro di Sicurezza Nazionale Cibernetica conferisce all'ecosistema per la sicurezza cibernetica del nostro Paese un carattere *"olistico"*, estendendo le indicazioni di carattere tecnico, organizzativo e procedurale per l'innalzamento dei livelli di sicurezza cibernetica di reti e sistemi (ispirate al Framework Nazionale per la Cyber Security e la data Protection[10]), anche a quelle società ed enti pubblici e privati non ricompresi nella Direttiva NIS, che hanno un rapporto con le funzioni essenziali dello Stato e la sicurezza nazionale; in altre parole, il Perimetro Nazionale di Sicurezza Cibernetica, sfruttando un principio di complementarità alla Direttiva NIS, estende e rafforza più in generale la capacità di difesa "cyber" del Sistema Paese.

Posizionato il Perimetro di Sicurezza Nazionale Cibernetica nell'ambito della nostra strategianazionale di cyber security, illustriamo, se pur in maniera sintetica, i punti salienti che lo caratterizzano ed in particolare:

1 entro 4 mesi dall'entrata in vigore della legge di conversione, saranno individuati, con uno specifico DPCM, i soggetti appartenential perimetro stesso. I criteri per individuarequesti soggetti sono già stati in parte citati, dunque tutti quelli che esercitano una funzione essenziale per lo Stato attraverso l'uso di reti, sistemi informativi e servizi informatici che possano pregiudicare in determinate condizioni la sicurezza nazionale, tenendo comunque conto di un principio di gradualità in relazione alle specificità dei diversi settori di attività. Tra i loro principali obblighi vi sarà la redazione, con cadenza annuale, da trasmettere alla Presidenza del Consiglio e al Ministero dello Sviluppo Economico per competenza, di un elenco delle proprie reti, dei sistemi informativi, dei servizi informatici di pertinenza, comprensivi dell'architettura e dei componenti. I

ciriteri a cui dovranno ispirarsi i soggetti individuati per redigere tali elenchi, saranno definiti sempre nello stesso DPCM, e dal momento della sua entrata in vigore, la trasmissione dovrà avvenire entro e non oltre i 6 mesi. Gli elenchi saranno altresì resi disponibili al Dipartimento per la Sicurezza delle Informazioni al fine di attuare programmi di prevenzione delle reti, dei sistemi informativi, dei servizi informatici, nonché la preparazione e la gestione delle crisi che verrà affidata al Nucleo per la Sicurezza Cibernetica.

2 entro dieci mesi dall'entrata in vigore della legge di conversionei soggetti individuati dovranno comunicare al CSIRT Italiano gli incidenti informatici aventi impatto rilevante sulle funzioni essenziali dello Stato e la Sicurezza Nazionale. Il CSIRT a sua volta informerà il Dipartimento per la Sicurezza delle Informazioni e dunque il Nucleo di Sicurezza Cibernetico per le attività di competenza; analogamente, nei suddetti tempi, saranno stabilite le misure di sicurezza volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici, ciò tenendo conto degli standard definiti a livello internazionale e dell'Unione europea. Nel caso particolare, in cui un soggetto appartenente al Perimetro Nazionale di Sicurezza Cibernetica sia anche un operatore di servizi essenziali già soggetto ai vincoli della Direttiva NIS, dovrà continuare ad adottare tutti i provvedimenti ed i comportamenti stabiliti da tale normativa, aggiungendovi quanto necessario per soddisfare gli ulteriori requisiti emanati nell'ambito del Perimetro stesso.

3 i soggetti appartenenti al perimetro, qualora dovessero affidare forniture di beni, sistemi e servizi ICT destinati ad essere impiegati su reti, sistemi informativi e per l'espletamento dei servizi informatici essenziali per lo Stato e/o per erogare servizi critici per lo Stato, dovranno informare tempestivamente e preventivamente il Centro di Valutazione e Certificazione Nazionale, il c.d. CVCN presso l'Istituto Superiore della Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico[11], rilasciando contestualmente la valutazione del rischio associato all'oggetto della fornitura e all'ambito di impiego. Con tempistiche definite, il CVCN potrà svolgere verifiche preliminari ed imporre condizioni e test, hardware e software, da compiere anche in collaborazione con il soggetto segnalante, secondo un approccio gradualmente crescente nelle verifiche di sicurezza. Ai fini della verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità note, anche in relazione all'ambito di impiego, il CVCN definirà le metodologie da adottare, avvalendosi anche di laboratori dallo stesso accreditati. Poiché la fase del *"procurement"* è delicata per qualsiasi impresa, a prescindere dalla sua natura e per favorirneil processo, decorso il termine previsto dalla legge senza che il CVCN si sia pronunciato, i soggetti che hanno effettuato la comunicazione potranno proseguire nella procedura di affidamento. Lo stesso articolo disciplina però anche il caso in cui il CVCN interviene direttamente. I bandi di gara infatti dovranno essere integrati con clausole che condizionano, sospensivamente ovvero risolutivamente, il contratto al rispetto delle condizioni e all'esito favorevole dei test disposti dal CVCN stesso. Anche le tempistiche per effettuare e concludere i test sono disciplinate in maniera rigorosa e ancora una volta con l'obiettivo di non rendere esasperante la procedura di *"procurement"*. In generale per particolari forniture di beni, sistemi e servizi ICT da impiegare su reti, sistemi informativi e servizi informatici del Ministero dell'Interno e del Ministero della Difesa che possono essere pregiudizievoli per la sicurezza nazionale, questi informeranno i propri centri di valutazione accreditati che utilizzeranno per le proprie valutazioni comunque le metodologie rilasciate dal CVCN;

4 saranno estesi i poteri speciali del Governo nei settori ad alta intensità tecnologica (Golden Power), con l'obiettivo di rendere i servizi erogati sulle reti di quinta generazione conformi agli standard di sicurezza il più possibile elevati. Del resto, sono stati condotti diversi studi sulla tecnologia 5G e il fatto che essa possa rappresentare una concreta minaccia rappresenta una oggettività condivisa; al riguardo proprio la Commissione Europea ha recentemente evidenziato tale criticità[12] pubblicando una relazione sulla valutazione coordinata a livello di UE dei rischi a cui è soggetta questa tecnologia in riferimento alla sicurezza cibernetica (minacce, vulnerabilità, ecc.). Tra l'altro è bene ricordare che, il 5G, dirompente sui mercati, è da considerarsi un fattore abilitante per molte altre tecnologie come ad esempio l'IoT, i Big Data, l'Intelligenza Artificiale, ecc.;

5 il Presidente del Consiglio dei Ministri, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici più volte precedentemente citati, potrà disporre, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico rischio o alla sua mitigazione, la disattivazione totale o parziale di apparati o prodotti utilizzati nelle reti, nei sistemi o per l'espletamento dei servizi interessati.

Conclusione

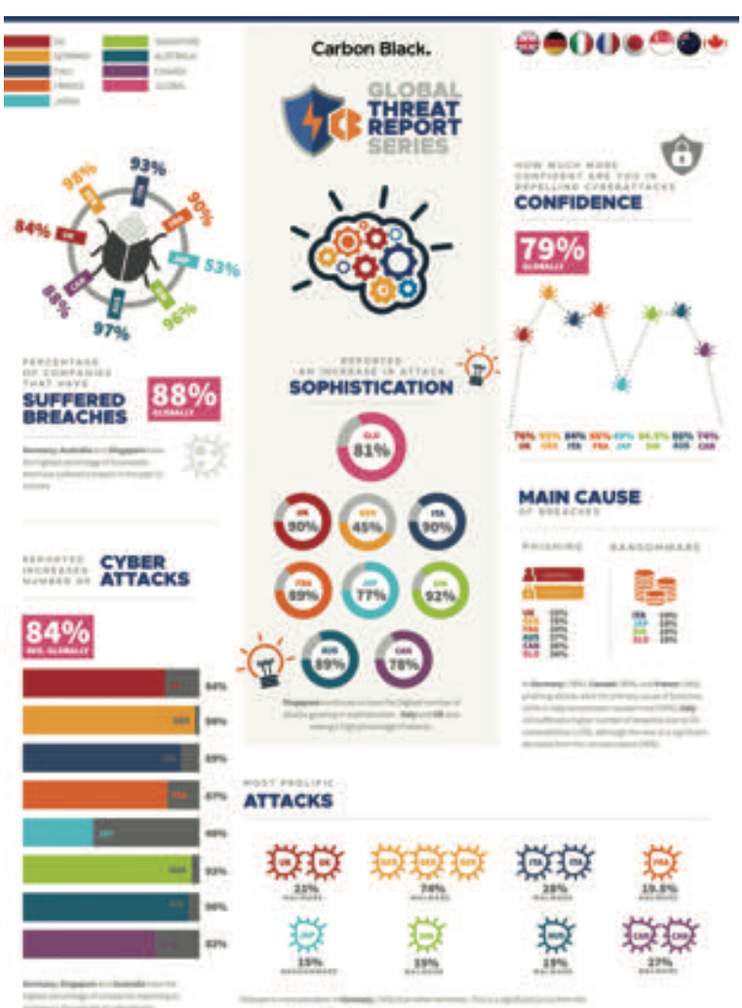
Con l'istituzione del Perimetro Nazionale di Sicurezza Cibernetica si chiude dunque un cerchio rimasto aperto con una previsione obblighi di innalzamento della sicurezza dei servizi estensiva anche verso tutti quegli operatori che, pur non essendo formalmente ricompresi tra quelli per l'erogazione di servizi essenziali e censiti secondo i criteri standard stabiliti a livello europeo dalla Direttiva NIS, purtuttavia svolgono un ruolo cruciale per la sicurezza stessa del Paese e dovrebbero pertanto garantire livelli ancora più elevati di sicurezza. ■

1 https://www.cybertrends.it/cybersecurity-act-un-nuovo-tassello-nella-strategia-cyber-sec-dellunione-europea/
2 https://www.gazzettaufficiale.it/eli/id/2019/11/20/19G00140/sg
3 sottolineato, quanto modificato con la conversione in legge
4 https://www.csirt-ita.it/
5 https://www.certnazionale.it/
6 https://www.cert-pa.it/
7 Nella figura non è rappresentato il caso di quegli operatori e servizi che, pur essendo funzionali al mercato, ai cittadini e alla società in generale, rivestono un ruolo strategico per la sicurezza dello Stato e la Sicurezza Nazionale.
8 Direttiva (UE) 2016/1148 del Parlamento Europeo e del Consiglio, Art. 1, "La presente direttiva stabilisce misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento delmercato interno"; analogamente il d.lgs.18 maggio 2018, n. 65, con il quale si recepisce la Direttiva in Italia, all'art. 4 ricorda che tra i criteri per l'identificazione degli operatori di servizi essenziali c'è quello per cui il soggetto deve fornire un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali.
9 d.l. 21 settembre 2019, n. 105, Art.1, "Al fine di assicurare un livello elevato di sicurezza dellereti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali,pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali oeconomiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale,è istituito il perimetro di sicurezza nazionale cibernetica."
10 https://www.cybersecurityframework.it/
11 https://www.mise.gov.it/index.php/it/per-i-media/notizie/it/198-notizie-stampa/2039261-istituito-il-centro-di-valutazione-e-certificazione-nazionale-cvcn
12 https://ec.europa.eu/commission/presscorner/detail/it/IP_19_6049

Intervista VIP a Rick McElroy, Responsabile Cyber Strategy, CARBON BLACK

Rick McElroy

Autore: Elena Mena Agresti



Quale scenario gli esperti della cyber security si devono preparare ad affrontare? Carbon Black ha recentemente pubblicato il secondo Threat Report dedicato all'Italia per comprendere le sfide e le problematiche che le imprese italiane si trovano a dover affrontare in un contesto nel quale gli attacchi informatici continuano a intensificarsi.

Di certo saranno necessari una maggiore automazione, intelligenza artificiale e strumenti che offrano una visibilità completa di reti complesse ed in continua evoluzione. L'efficienza delle risorse diventerà la parola d'ordine poiché le aziende mirano a massimizzare la capacità dei team di rilevare e mitigare le minacce e a investire in modo intelligente negli strumenti che consentono ai loro team di costruire una crescente fiducia e gestire una difesa informatica proattiva.

Secondo i risultati del nostro secondo Rapporto sulle minacce informatiche in Italia, le aziende si stanno adattando alla "nuova normalità" di attacchi informatici continui e sofisticati. Una maggiore consapevolezza delle minacce esterne e dei rischi inerenti alla conformità ha inoltre spinto le imprese a diventare più proattive nella gestione dei rischi informatici, via via che assistono agli impatti finanziari e reputazionali provocati dalle

violazioni. Il rapporto ha rilevato che il 93% delle imprese italiane interpellate ha subito delle violazioni negli ultimi 12 mesi; fra queste, il 43% ha registrato da 3 a 10 violazioni.

Via via che il settore della difesa alla pirateria informatica continua a maturare, le aziende stanno diventando più consapevoli degli strumenti a loro disposizione e delle tattiche che possono usare per combattere gli attacchi informatici. Riteniamo che questa crescente fiducia sia indicativa di un cambiamento di potere a favore dei *cyber defender*, che stanno adottando un approccio più proattivo al *Threat Hunting* e alla neutralizzazione delle minacce rispetto al passato.

La superficie è aumentata esponenzialmente ma è bene fare una distinzione tra produttori e consumatori.

Se è vero che i produttori sono sempre più preparati e pronti, i consumatori non lo sono e proprio per questo è necessario iniziare a pensare ad una politica di *shared security*. Una sicurezza che deve necessariamente valutare tutti gli ambiti specialmente per realtà che hanno difficoltà a comprendere la sicurezza informatica.

Emerge, infatti, un gap generazionale nel quale oggi le generazioni meno giovani si trovano al di fuori delle logiche di sicurezza informatica e delle *best practice* informatiche per difendersi.

Credo che solo tra 40 anni arriveremo ad una generazione completamente matura in grado di approcciare al meglio questa *digital transformation*.

Nuove tecnologie possono essere di supporto alle attività dei team di sicurezza?

La blockchain sicuramente è una nuova tecnologia che può garantire enormi vantaggi. Uno di questi è la garanzia dei certificati dei singoli nodi. Tuttavia non è, a mio avviso, applicabile a tutti i settori. Alcuni settori devono continuare a lavorare nella direzione con la quale stanno lavorando implementando le tecnologie di sicurezza quali IDS, IPS, SIEM etc. Un esempio di applicazione di successo che deve essere portato alla luce è sicuramente l'applicazione della blockchain ai sistemi SWIFT. Sebbene sia complesso il perimetro di tale sistema, la blockchain potrebbe avere un importante ruolo nel garantire la sua sicurezza.

Intelligence Artificiale e Machine Learning sono degli strumenti rivoluzionari per la cyber security così come il 5G rappresenta il futuro delle comunicazioni.

Dalla ricerca condotta in Italia emergono notevoli preoccupazioni dei professioni della sicurezza circa i progetti di trasformazione digitale e l'implementazione del 5G e che influenzeranno la loro posizione di rischio.

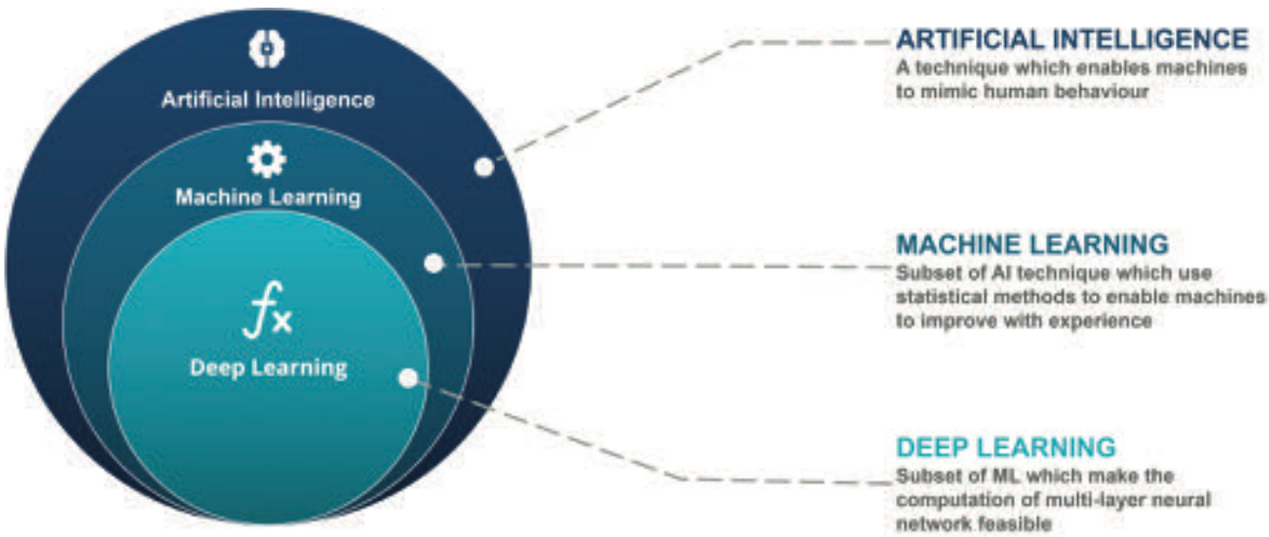
BIO

Rick McElroy, Responsabile della Security Strategy per Carbon Black, ha più di 15 anni di esperienza nella sicurezza delle informazioni nell'educare e supportare le organizzazioni nella riduzione della loro esposizione al rischio e nell'affrontare le difficili sfide di sicurezza. Ha ricoperto posizioni di sicurezza presso il Dipartimento della Difesa degli Stati Uniti e in diversi settori, tra cui retail, insurance, intrattenimento, cloud-computing e istruzione superiore. L'esperienza di McElroy spazia dall'esecuzione di penetration test alla definizione e conduzione di programmi di sicurezza. È certificato CISSP), CISM,CRISC. Come marine degli Stati Uniti, il lavoro di McElroy includeva servizi di sicurezza fisica e antiterrorismo. Un feroce difensore della privacy e della sicurezza, richiede che l'istruzione e l'innovazione siano le chiavi per migliorare il panorama della sicurezza, McElroy è presidente del programma per il CyberFest annuale della Securing Our eCity Foundation , un evento di San Diego dedicato all'educazione alla sicurezza del settore pubblico e privato e ai professionisti IT e ai dirigenti delle aziende sulle realtà della sicurezza.

Il 32% degli intervistati teme che il 5G creerà maggiori possibilità di esposizione agli attacchi informatici.

Si parla molto del 5G e i rapporti con la Cina. Cosa ne pensa?

Viene sottolineato da molti come le tecnologie 5G abbiano dei costi decisamente minori potendo rappresentare una minaccia per i paesi dell'occidente. Tuttavia se si prende come dato di fatto il timore di essere spiati e non poter far nulla a riguardo data la provenienza delle tecnologie implementate nelle infrastrutture è necessario agire in altro modo. È di fondamentale importanza un controllo e una difesa più prossima che tenga conto che esiste un problema a monte, ovvero le tecnologie fornite per l'appunto. L'autenticazione a due fattori o altri metodi di autenticazione sono sicuramente uno degli elementi che possono venirci in aiuto. Vorrei aggiungere che il 5G, oltre a rappresentare il futuro delle comunicazioni, gioca un ruolo di geopolitica molto importante e difficile da poter prevedere. Molto dipende dalle volontà dei singoli Stati e dalle decisioni politiche che adottano nei propri ordinamenti.



Ha definito l'Intelligenza Artificiale e il Machine Learning strumenti rivoluzionari. Ma qual è il ruolo dell'uomo?

L'Intelligenza Artificiale e il Machine Learning offrono ovviamente un ampio margine di miglioramento nell'analisi dei dati ma non dobbiamo dimenticarci che tutti i giorni le più grandi società di sicurezza informatica si confrontano con altri soggetti altrettanto "umani".

Proprio l'aspetto umano è fondamentale. Studiare i trend, i comportamenti, le dinamiche che l'uomo mette in campo per superare le barriere di protezione messe a disposizione, è la chiave del successo. L'Intelligenza Artificiale e il Machine Learning ci possono aiutare in tal senso, specialmente per tutti quei fenomeni "anormali" ai quali probabilmente non si pensa, ma che esistono. Ripeto l'uomo e gli attaccanti al centro. Si veda una macchina IA. È bellissimo poter dormire e non dover guidare ma è bene pensare che dietro l'auto c'è un uomo!

Un tema di forte discussione è il rapporto tra endpoint e cyber insurance.

Un frigo, una automobile devono essere pensati e costruiti per essere sicuri perché è invitabile che il consumatore possa incorrere in errori. Ecco perché le società che si occupano di sicurezza informatica devono essere sempre pronte ad affrontare qualsiasi tipo di minaccia.

In caso di attacco informatico portato a segno, trovo però particolarmente complesso poter dimostrare l'inefficacia di una soluzione di sicurezza applicata. Questo perché esistono forme di attacco sempre nuove ed è difficile poter tipizzare la tipologia di attacco e di danno, giuridicamente parlando. A questo bisogna aggiungere che le assicurazioni e cyber insurance non hanno definito uno standard o un framework degli schemi risarcitori prestabiliti o fattispecie tipizzate come magari avviene per gli incidenti auto. Sappiamo che, dato un evento, un tamponamento ad esempio, l'assicurazione coprirà il danno qual ora sussistano le condizioni stabilite nel contratto. Contrattualizzare tutti gli eventi, e quindi i danni che possono scaturire da un cyberattacco è complesso.

E se l'attaccante è un attore governativo?? Le ultime cyber insurance prevendono una clausola di manleva per gli attacchi governativi. Come potremmo mai dimostrare che l'attacco subito è stato scagliato da un governo piuttosto che da un altro attore?

La privacy e l'etica del digitale sono tematiche in continua evoluzione. Molte informazioni in passato erano considerate più sensibili di oggi. Pensa che in futuro saranno ancora rilevanti o meno?

E' fondamentale avere un approccio costruttivo alla privacy e imparare a comportarsi secondo privacy. Quando ho detto a mio figlio che molto probabilmente il governo stava spiando il suo telefono, mio figlio non ha battuto ciglio, come se non gli importasse. Quando gli ho chiesto di farmi vedere i suoi messaggi privati, le sue foto, il suo profilo Instagram, ecco allora si è infervorato e mi ha risposto di no.

Questo è un riassunto di come oggi si vive la privacy bisogna essere consapevoli che è un elemento importantissimo a prescindere da chi sia l'interlocutore se un sito, una terza parte etc. Cambridge Analytica è stato un classico esempio. Ha impattato privati, aziende e elezioni di una nazione.

Dal lato tecnologico è importantissimo poter approcciare questo tema by design e by default. I sistemi anche a fronte delle nuove normative, internazionali ed europee a garanzia del dato personale non posso tralasciare questo aspetto fondamentale!!!

Parlare di etica al giorno d'oggi è importante e fondamentale. Credo che assisteremo ad una evoluzione delle figure umanistiche nel settore tecnologico e dell'informatica. Mentre l'informatico ha un approccio diretto alla tecnologia, al problema, alla risoluzione del problema, l'umanista valuta altri fattori, anche morali che necessariamente devono essere presi in considerazione. Sarà complesso gestire lo scenario che ci attende, per esempio dare priorità alle scelte che una macchina basata su Intelligenza Artificiale dovrà fare e proprio per questo servirà il supporto dell'uomo pensante. ■

Recensione di: Mariana Mazzucato, Il Valore di tutto: chi lo produce e chi lo sottrae nell'economia globale, Laterza 2019

Autore: Massimiliano Cannata

Privato o pubblico: chi innova di più?

Esiste una macchina dello stato diversa, da come ce lo hanno sempre raccontato, sprecona, lenta, burocratizzata. Non è vero che tutto ciò che è pubblico va considerato di serie B, da annoverare nell'orizzonte del parassitismo, il soggetto pubblico può, infatti essere, un importante catalizzatore di trasformazioni, in grado di imprimere un indirizzo allo sviluppo, come dimostra la storia di Paesi oggi all'avanguardia nel mondo per indici di crescita e per investimenti nella ricerca.

Per comprendere questo bisogna prima di tutto andare contro luoghi comuni e resettare convinzioni ossificate nel tempo, frutto di incrostazioni e ignoranza. **Mariana Mazzucato**, nota al grande pubblico per "Lo stato innovatore" tradotto in Italia da Laterza qualche anno fa, docente di economia *dell'Innovazione all'University College London*, dove ha fondato un istituto per l'Innovazione e il valore pubblico, ha imboccato questa strada ancora poco battuta da economisti e studiosi, per approdare a una conclusione molto chiara: è lo Stato il primo motore del cambiamento, non l'impresa privata. Nel suo ultimo saggio *"Il Valore di tutto: chi lo produce e chi lo sottrae nell'economia globale"* (ed. Laterza) la studiosa argomenta questa tesi, offrendo un'analisi attenta e originale del concetto di valore. Con esempi alla mano il lettore può comprendere quanta ambiguità e confusione viene fatta, anche dagli operatori dell'informazione, quando viene utilizzato questo termine – chiave per comprendere le dinamiche che regolano l'economia e della finanza.

"Molti dei cosiddetti creatori del valore dell'industria tecnologica – si legge nella prefazione - attaccano i governi considerandoli un puro impedimento alla creazione di valore. A cominciare da **Eric Schimdt** amministratore delegato di Google che ha ripetutamente dichiarato che i dati dei cittadini sono più sicuri con la sua azienda che con ilgoverno. Tale affermazione riflette un tradizionale retaggio (consolidatosi verso la metà degli anni ottanta quando è trionfata la visione neo - liberista fondata su una cieca fiducia nei poteri del mercato) secondo cui gli imprenditori sono buoni, mentre il governo è cattivo, quando non inetto". Affermazione palesemente errata, precisa con ricchezza di argomentazioni l'autrice, basta riflettere sulla provenienza di quelle tecnologie all'avanguardia che oggi alimentano la cosiddetta rivoluzione digitale: Internet, GPS, il *touch screen*, SIRI, algoritmo di Google, tutti strumenti finanziati da istituzioni pubbliche.

Stop alle cattive favole

Uno sbaglio simile, quello commesso da Apple, che ha recentemente dichiarato di non voler pagare le tasse, in virtù del ruolo pionieristico svolto sul terreno dell'innovazione. Curiosa posizione se si tiene conto che sarebbero invece i contribuenti a dover pretendere qualcosa in cambio, quei contribuenti che, da utenti finali, sono invece sistematicamente *tartassati* (Totò nella nota pellicola del 1959 aveva capito già tutto n.d.r.) da balzi e balzelli, che erodono il potere d'acquisto, deprimono la domanda, creando fatalmente i presupposti della crisi.

Troppe cattive favole, girano evidentemente attorno al ruolo e alla funzione dello stato. La Mazzucato, ricorrendo a una citazione aulica, richiama Platone, precisamente il passo de La Repubblica in cui vengono denunciati i creatori di quelle false narrazioni (*fake news ante litteram* le potremmo definire n.d.r), che servono a governare il mondo. Non è cambiato nulla verrebbe da dire, rispetto alla Grecia del V secolo a.C. . Anche oggi come ieri, infatti, esiste una "fabbrica" della falsificazione che crea illusioni ottiche, finendo col condizionare le classi dirigenti (almeno qui non c'è da fare distinzione tra pubblico e privato) chiamate a operare delle scelte decisive per il futuro di popoli e nazioni.

Chi crea e chi estrae valore

Per correggere il tiro occorrerà imparare in fretta a "leggere" la differenza tra chi crea realmente valore e chi invece estrae valore, giovandosi di grandi profitti, che non hanno nessun ritorno per la collettività. Il caso della Goldman Sachs, richiamato nel libro, il cui crollo nel 2008 ha, come è noto, contribuito a generare la peggiore crisi economica della storia dagli anni 30 è emblematico. Solo un anno dopo, nel 2009, l'amministratore delegato *Lloyd Blankfein* come se nulla fosse successo, si spinse a dichiarare con solennità che i suoi dipendenti erano tra i più produttivi al mondo, dimenticando un particolare: erano stati i contribuenti a pagare ben 125 miliardi di dollari per salvare l'azienda; vicenda non dissimile era toccata allo stato americano, che fu costretto ad accontentarsi di recuperare a mala pena i quattrini investiti per rimettere in sesto un sistema bancario, ormai al collasso.

Se il mito del privato, dunque, vacilla è venuto il momento di riconsiderare il ruolo che il pubblico può avere in un moderno ecosistema della crescita. Nessun facile ottimismo, per carità, semmai un esercizio di consapevolezza e responsabilità nel considerare la funzione strategica che rivestono attori istituzionali e soggetti privati; questo il messaggio forte che emerge da tutta l'opera della Mazzucato, che apre con il suoi lavori, dei percorsi importanti per l'analisi e l'approfondimento.

La parterschip pubblico privato e la svolta Green

"Non possiamo continuare a utilizzare occhiali vecchi", ma attenzione, aggiungiamo: bisogna inforcare la montatura giusta, perché lo stato assuma i giusti contorni di stimolatore dell'innovazione, senza soffocare la libertà dell'impresa privata, né tantomeno sostituendosi ad essa. Stiamo parlando di equilibri sottili certo, su cui il dibattito economico non a caso si confronta da

secoli. Guardando all'attualità risulterà decisiva la collaborazione tra pubblico e privato che per l'Italia, ancora molto indietro su questo terreno, potrebbe già rappresentare un'occasione importante per cominciare a voltare pagina.

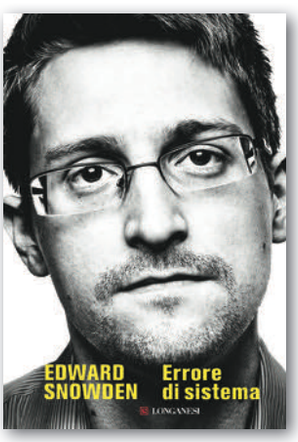
Altro aspetto essenziale l'innalzamento del livello dei manager e dei tecnici che operano nel settore pubblico. Senza, un investimento forte nel capitale umano sarà difficile imboccare percorsi virtuosi per la pubblica amministrazione, chiamata a mettere ordine al sistema delle concessioni, e a impegnare risorse dirette nelle banche pubbliche, nella Cdp, e negli stessi enti pubblici perché il volano della ripresa possa prendere linfa.

Occorre una dirigenza pubblica illuminata, abituata a gestire e non a stare alla finestra. Il recente annuncio del neo ministro Fabiana Dadone, di una svolta green, le cui tracce sono visibili anche nella finanziaria che andrà al vaglio delle Camere, richiederà una capacità di valutare gli impatti sociali delle politiche pubbliche, competenza tutta da costruire e affinare. Energia rinnovabile, materiali diversi, infrastrutture moderne rispettose dell'ambiente, *green* è una parola polisemica, vuol dire tante cose, soprattutto una profonda trasformazione tutti i settori dell'economia, dall'industria ai compresi i servizi. Il nostro Paese, se gli intendimenti del Ministro troveranno attuazione, potrebbe fare un sensibile scatto in avanti.

In conclusione non si tratta di "tifare" per uno stato leggero, perché deve pur sempre avere componenti e fattori di qualità al suo interno per rimuovere con prontezza gli ostacoli che a vari livelli frenano l'innovazione. Piuttosto, volendo interpretare la posizione della Mazzucato, dovremmo parlare di uno stato e di una PA, arbitro e "imprenditore" intelligente, attento custode delle regole. Solo a queste condizioni, superando il "bagno ideologico", impegnativa eredità di un passato neanche troppo lontano, si potranno gettare le basi per un piano strategico di ripresa dell'economia che possa presentare una forte missione pubblica, lasciandosi finalmente alle spalle l'atmosfera cupa di questi lunghi anni di crisi. ■

Recensione a Edward Snowden, Errore di sistema, Longanesi, 2019

Autore: Massimiliano Cannata



Alt al capitalismo della sorveglianza

Edward Snowden, funzionario presso agenzie di intelligence e di sicurezza informatica, presta servizio presso la CIA e la NSA, a un certo punto… succede qualcosa un cambio di vita e di prospettiva. Edward decide, come - spiega nella prefazione di "Errore di sistema" (ed. Longanesi) "di lavorare per le persone, non più per i governi. Dovevo cercare – confessa nel racconto che è già un best seller mondiale – di proteggere i cittadini da quello che avevo contribuito a creare, un sistema di spionaggio di massa, capace di sorvegliare i movimenti di tutti. Nulla di simile era mai esistito nel passato".

Bisogna riavvolgere il nastro per comprendere meglio il contesto di riferimento, e risalire all'11 settembre. Dopo il tragico attentato Il mondo era cambiato, gli USA, super potenza per eccellenza, erano stati feriti al cuore. Quell'onta doveva essere cancellata, per evitare che l'irreparabile si potesse ripetere. Da quel momento la tecnologia entra nei sistemi organizzativi e nei palazzi di governo, i tecnici informatici per la prima volta pesano di più degli scienziati della politica, prendono in mano le redini della situazione, finendo col condizionare, con il loro operato, scelte strategiche e decisioni vitali per gli equilibri del pianeta. Conoscere bene un PC, nel nuovo scenario sconvolto dal terrorismo globale, equivale a possedere una laurea specialistica. In virtù di questa competenza la stessa carriera di Snowden si evolve rapidamente bruciando le tappe. Inutili diplomi e "pezzi di carta", anche agenzie americane decidono di derogare a qualsiasi regola, la cosa più importante risiede nel dimostrare di avere dimestichezza con le macchine intelligenti, considerato che la sicurezza e la tenuta stessa delle democrazie dipende, in maniera decisiva, dal buon funzionamento di apparati e sistemi elettronici.

Nel breve volgere di pochi anni da quel fatidico 2001 l'attività di intelligence muta il suo profilo. così, il suo profilo. Dagli incontri clandestini ai dati il salto è grosso. Quello che racconta l'autore è un cambio di paradigma, non semplicemente la storia di un'esperienza personale e di un percorso lavorativo. Digitalizzare il sistema di spionaggio, far entrare la tecnologia dentro i paludati e segreti ambiti della diplomazia, non era più un'eresia, una sorta di profanazione di territori prima di allora insondabili, ma una nuova forma di organizzare i saperi e le competenze. Lo scenario dei *big data* diventa progressivamente il brodo di coltura entro cui viviamo immersi, la società automatica, per usare una fortunata definizione di Bernard Stiegler, poteva celebrare una prima roboante conquista: quella della softwarizzazione globale: nessun angolo dell'esistenza sarebbe potuto sfuggire all'osservazione e al controllo.

Il potere dell'algoritmo

Potere dell'algoritmo si potrebbe dire, alimentato dall'utopia della perenne duplicazione automatica delle nostre azioni. Siamo dentro un'immensa architettura reticolare che contiene tutto, non esiste un "di fuori", neanche una crepa apparente, l'uno-tutto di questa straordinaria macchina è una manifestazione di un universo mutante, fatto di informazioni. L'automatismo che lo attraversa giustifica se stesso, si autoalimenta, spinto da una possente bulimia, ingoia dati su dati, senza una trama di senso. Ed è su questo "vuoto di significato" che si insinua il tarlo del dubbio: "Avevo lavorato per creare un meccanismo di conservazione della traccia permanente di ciascuno di noi, non immaginavo che errore grande potesse essere". Come spesso accade è nelle situazioni più imprevedibili che scatta qualcosa: l'autore si trova nel paradiso delle Hawaii, in un luogo "oltre", fuori dalla solita quotidianità, lì viene colto dalla sensazione di aver sbagliato strada. Da quel lontano angolo del

mondo era maturata una consapevolezza nuova: la gigantesca macchina creata poteva servire a spiare la vita di milioni di persone, una violazione gravissima dei diritti fondamentali, affermati nella carta costituzionale americana che sono poi alla base di ogni società libera, era stata pensata e, ancor peggio attuata.

Tolto il "velo di maya" della finzione, che nel caso di Snowden per sua stessa ammissione si poteva definire *"need-to-know"* occorreva guadagnare una visione diversa della realtà e delle cose, e chiedersi: Esiste un argine possibile rispetto alla pericolosa deriva del controllo pervasivo e costante degli individui in ogni angolo del pianeta? La tutela del corpo fisico e del corpo elettronico, come lo definiva il grande giurista Stefano Rodotà, è ancora perseguibile? Che significato possiamo dare all'errore (concetto fondamentale per la ricerca scientifica recentemente rivalutato da un bellissimo saggio - dialogo che il filosofo della scienza Giulio Giorello intrattiene con Pino Donghi ed. Il Mulino), che un atteggiamento acriticamente fideistico ci aveva fatto rimuovere dal nostro interesse e dalla nostra analisi? Se le parole ancora valgono, come un recente grande evento internazionale organizzato della Treccani ha puntualizzato, tra queste "verità" torna a occupare un posto importante, quando sembrava ormai passato di moda, smarrito nel labirinto di una crisi culturale e filosofica, prima che sociale e politica. Il racconto di Snowden scaturisce da un desiderio di verità, valore in totale contrasto con quanto prescriverebbe il suo mestiere come il suo. La stampa di tutto il mondo doveva sapere.

La verità primo motore della narrazione

Nasce così "Errore di sistema", un libro affascinante, rivolto ai lettori di tutto il mondo, che puntualizza la centralità delle speranze e dei valori, che devono rimanere al di sopra, a dispetto delle convinzioni dei più, della ricchezza e dei guadagni. La denuncia di questo genio dell'informatica investe più ambiti chiamando in causa tutta una generazione che aveva creduto nella Rete, come piattaforma di relazione e di incontro, strumento eccezionale di intelligenza collettiva. Un sogno infranto ormai, mentre si fa sempre più strada un capitalismo della sorveglianza con il conseguente crollo del web creativo. Oggi bisogna impegnarsi a fondo perché questa "mutazione" della Rete, possa essere ricondotta nell'alveo del diritto di ciascun uomo di essere libero di pensare e di agire, in ogni parte del pianeta si trovi a vivere.

Libertà e sicurezza devono trovare un punto di equilibrio, questo l'insegnamento che proviene dalla coraggiosa esperienza di Snowden. "La libertà di un Paese deve esser misurata nel rispetto dei diritti di ogni cittadino, perché sono questi diritti che rappresentano la restrizioni all'eccessivo potere dello Stato". Per quei diritti generazioni di donne e uomini si sono sacrificati, tocca a noi raccogliere quell'impegnativo lascito, riconoscendoci in perenne "lotta per la verità" che, anche nella civiltà delle macchine, si identifica con un tendere verso, un andare oltre che non deve mai tradire la forza autentica dell'origine.

In questi anni, si legge nella biografia ufficiale, sono stati tributati prestigiosi riconoscimenti per l'impegno di Edward Snowden a favore della libertà e dei diritti dell'uomo, tanto che attualmente il nostro autore è Presidente del Consiglio di Amministrazione della *Freedom of the press Foundation*. Evidentemente si può ancora sperare in un mondo migliore, senza dover necessariamente uscire sconfitti da un sistema, che di errori e di debolezze ne ha, probabilmente, più di uno. ■

Recensione a: Shoshana Zuboff, Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri. Roma (Luiss), Ottobre 2019, 622 pagine

Autore: Laurent Chrzanovski

"Ogni nostra email, ogni nostra interazione, ogni nostra emozione è venduta, controllata, manipolata. Mai la società umana ha avuto una così grande concentrazione di ricchezza, conoscenza e potere in così poche mani. Non ve ne siete accorti? Leggete Shoshana Zuboff."
Roberto Saviano

Sin dalla sua prima edizione statunitense a gennaio di questo anno, ad opera della prestigiosa casa editrice Public Affairs *(The Age of Surveillance Capitalism. The Fight for a Human Future at the new Frontier of Power)*, il capolavoro di Shoshana Zuboff è già entrato a far parte del pantheon dei libri che costituiscono la pietra angolare della comprensione di base dell'ecosistema digitale che il mondo intero utilizza quotidianamente.

Redigere una recensione su quello che può essere definito un vero e proprio manuale di comprensione e sopravvivenza è un esercizio estremamente arduo. Dalla settimana successiva al suo lancio, il mondo della ricerca e dei media - dai più specialistici ai più generalisti - hanno prodotto una quantità di testi dedicati all'analisi della Zuboff.

Per i lettori italofoni, sottolineeremo le profonde riflessioni scritte da Mario Mancini (1) da Maurizio Franzini (2) e da Hamilton Santia (3), veri e propri saggi offrono approfondimenti nonché letture supplementari e quindi meritano di essere letti come tali, accanto ai quali spicca, come introduzione alla lotta per salvare i nostri valori nel mondo si sorveglianza, l'eccellente intervista-recensione, in presenza dell'autrice, ad opera di Géraldine Delacroix e subito proposta in traduzione italiana a cura di Salvatore Pallida (4).

Prima di partire con un vero e proprio viaggio iniziatico «alla Prévert» – visto l'abbondanza di informazioni vitali contenute nel volume ed il piccolo spazio a noi riservato, bisogna subito sottolineare che l'autrice è, come specialista, una vera e propria anomalia nel mondo odierno.

Bibliografia - Cybersecurity Trends

Professoressa emerita di Business Administration e poi membro del Berkman Center for Internet and Society, all'Università di Harvard, Shoshana Zuboff non è un avvezza a pubblicazioni annue di articoli scientifici di piccolo o medio taglio.

All'opposto, si è concentrata a scrivere soli 3 libri tutti immediatamente di successo sia per mondo universitario che il grande pubblico, fatto anch'esso rarissimo: *In the Age of the Smart Machine: The Future of Work and Power* (New York 1988), *The Support Economy: Why Corporations Are Failing Individuals and the Next Episode of Capitalism* (Londra 2002), e il volume del quale trattiamo oggi.

Scrittrice e divulgatrice senza pari, ha invece impiegato grande parte del suo tempo a spiegare le sue tesi ed a trattare per il grande pubblico temi di attualità tramite i migliori media. È possibile accedere a molti di questi saggi, interviste e conferenze sul sito dell'autrice: http://www.shoshanazuboff.com/).

Venendo al libro, lo scenario dipinto dalla Zuboff è presente, talvolta persino palpabile per chi è attento alle deviazioni del mondo digitale, e le sue conseguenze future sono drammatiche. Come lo scrive chiaramente, *"Siamo vittime di un'asimmetria senza precedenti: Il capitalismo di sorveglianza sa tutto di noi, mentre le sue operazioni sono progettate in modo che non ne sappiamo nulla, esso annulla i diritti fondamentali associati all'autonomia individuale, diritti essenziali per la possibilità stessa di una società democratica".*

La definizione proposta sin dall'inizio del libro lascia con molti brividi e senza parole:

"Ca-pi-ta-lis-mo di sor-ve-glian-za, n.

1 Un nuovo ordine economico che rivendica l'esperienza umana come materia prima gratuita per attività commerciali che nascondono pratiche di estrazione, previsione e vendita;

2 Una logica economica parassitaria in cui la produzione di beni e servizi è subordinata ad una nuova architettura globale di modificazione comportamentale;

3 Una mutazione canaglia del capitalismo segnata da concentrazioni di ricchezza, conoscenza e potere senza precedenti nella storia dell'umanità

4 Il quadro fondamentale di un'economia di sorveglianza

5 In quanto tale, una minaccia significativa per la natura umana nel ventunesimo secolo, come il capitalismo industriale era per il mondo naturale nel diciannovesimo e ventesimo secolo;

6 L'origine di una nuova potenza strumentale che afferma il suo predominio sulla società e presenta sfide sorprendenti per la democrazia di mercato

7 Un movimento che mira a imporre un nuovo ordine collettivo basato sulla certezza assoluta

8 Un esproprio dei diritti umani fondamentali, da intendersi come un colpo di stato venuto dall'alto: il rovesciamento completo della sovranità del popolo."

E' necessario sottolineare qui che Shoshanna Zuboff è stata la prima professoressa di Economia ad Harvard, che man mano, dalla fine degli anni ottanta, venne ad interessarsi al mondo digitale.

Non ci troviamo quindi di fronte all'ennesimo ma eccellente "whisleblowing book" di ex-insiders come *"I'm Feeling Lucky: The Confessions of Google Employee Number 59"* di Douglas Steward (New York 2011) e il recentissimo *"Zucked. Waking Up to the Facebook Catastrophe"* di Roger McNamee (New York 2019). Ben al contrario, siamo davanti ad un manuale universitario con più di 50 pagine di riferimenti bibliografici, col vantaggio enorme – ricetta del suo successo – di essere scritto col talento degno di un autore affermato di thriller.

Ogni frase, ogni concetto è sostenuto, argomentato, asciutto, rendendo l'argomentazione inattaccabile. E quindi ancora più grave.

Tralasciando i mille metodi di spionaggio comportamentale, che hanno reso ormai le majors in possesso quasi totale di tutta la nostra vita passata, presente e futura, e che costituiscono la maggior parte del volume, ci concentreremo sulle cause che hanno portato il pianeta intero in questa situazione.

L'abbandono totale delle autorità statali occidentali, ed in primis americane, vi è spiegata proprio da quella che fu professoressa di molti politici e CEO's di vari settori produttivi in modo magistrale: all'inizio, la tecnologia e la raccolta dei dati non erano stati percepiti come minacce. Non è stata capita né la sua folgorante capacità tecnica di miglioramento quasi quotidiano né tantomeno gli scopi sottostanti alla più grande raccolta di dati mai esistita nella storia. Ormai, il trend dettato, col consenso di chi immette dati sulla rete, dalle majors, non pare più contrastabile – soprattutto per paura delle élites politiche di essere considerate avvocati di un cattivo "deep State" simile a quello vissuto e denunciato da Edward Snowden – vedasi la recensione di Massimiliano Cannata sull'ultimo volume del collaboratore della NSA.

Zuboff rimette nel loro contesto espressioni del 2010, considerate allora come semplici dimostrazioni di ego e non percepite come apertura chiara alle ostilità. Spiccano in quell'anno l'intervista di Andy Grove, allora CEO di Intel, che dichiarò al Washington Post: *"High tech runs three-times faster than normal businesses. And the government runs three-times slower than normal businesses. So we have a nine-times gap… And so what you want to do is you want to make sure that the government does not get in the way and slow things down."*, che nonostante molte polemiche da parte delle élites intellettuali venne ribadita ancor più violentemente dal Eric Schmidt, allora CEO di Google: *"technology moves so fast that governments really shouldn't try to regulate it because it will change too fast, and any problem will be solved by technology. We'll move much faster than any government."*

Uomini d'affari, politici, economisti, non avendo la cultura necessaria e nemmeno esperti al loro fianco adatti a capire che era ancora possibile regolamentare e nello stesso tempo fare affari con le nuove tecnologie, preferirono allora, in modo ultra-liberale, accontentarsi della nuova manna che questi vari strumenti potevano portargli.

La situazione di oggi, come spiega Zuboff sia nell'introduzione che nella conclusione, impone una sola via a chi vuole essere libero: l'esilio. La propria abitazione, piena di ricettori - trasmettitori, "appartiene" già alle *majors*, e quindi neanche rifugiarsi in casa risulta più utile.

Con molta amarezza, vengono descritti i nativi digitali, per i quali la connettività dovrebbe essere "un diritto umano" ma senza

sorveglianza. Spiega bene che la loro libertà, allora, vuol dire rinunciare semplicemente ad esistere e vivere con mille maschere. Usando mezzi tecnologici speciali, maschere e abbigliamenti anti-ricognizione visuale, si può in effetti evadere "l'occhio di Dio" *(delle majors)*. Ma sono maschere che non si possono togliere, se non in luoghi ultra protetti. E' il nuovo campo – che imita quello militare – della *art and science of hiding*.

Le ultime pagine del volume sono un vero manifesto per una presa di coscienza civile ed un movimento sociale potente che, inevitabilmente, porterebbe i governi a prendere le misure politiche, strategiche e legali necessarie per evitare di cadere in *"un'era reazionaria in cui il capitale è autonomo e gli individui sono eteronomi; la stessa possibilità di sviluppo democratico e umano richiederebbe il contrario. Questo cupo paradosso è al centro del capitalismo di sorveglianza: un nuovo tipo di economia che ci reinventa attraverso il prisma del proprio potere".*

La proposta di Zuboff per salvare il salvabile: rimettere l'uomo al centro di un sistema culturale ed educativo performante permettendo a tutti i cittadini di capire l'ecosistema nel quale vivono, sulle altre proposte assistiamo a non pochi dibattiti in Europa.

E' proprio sul punto, basato sull'American way of life, dove l'individuo può far cambiare le cose e dove la società può salvare la democrazia, che si sono erette le più massicce critiche, *in primis* dai sociologi ma anche da vari *think tank* statali.

Le nostre leggi, le nostre libertà, le nostre cittadinanze sono infatti gestite da un patto sociale, basato non solo sull'opera omonima di Rousseau ma anche sulle realtà statati in vigore, ad iniziare dai servizi che lo Stato deve proporci a cambio dei nostri contributi, un assioma introdotto da Bismarck e continuato sino alla seconda guerra mondiale, assecondando perfettamente una filosofia ed un corpus giuridico continentale di stampo greco-romano, oggetto dell'ormai celebre *Come un ladro in pieno giorno. Il potere all'epoca della postumanità* di Slavoj Zizek (appena tradotto in Italiano, ed. Ponte alle Grazie, Milano 2019)

Per un lettore europeo, l'altro punto "debole" del libro della Zuboff, d'obbligo negli Stati Uniti di oggi dove ogni piccola distorsione al *"politically correct"* scatena uno tsunami di proteste, è di non accennare alla falsificazione e addirittura alla negazione, da parte dei GAFAM, della morale, della filosofia, della storia, della biologia e della sessualità, oggetto dell'ultimo saggio di Michel Onfray, recensito a seguito.

NB. La nostra recensione è stata eseguita utilizzando l'originale in lingua inglese. E' doveroso salutare la proattività della Luiss, permettendo agli italiani di essere tra i primi a poter usufruire di questo capolavoro nella propria lingua. Una piccola critica va però fatta alla libertà lasciata al traduttore. Il sottotitolo ne è un esempio lampante *"Il futuro dell'umanità nell'era dei nuovi poteri"* e non auspicato *"La lotta per un futuro umano alla nuova frontiera del potere",* come condurre questa "lotta" essendo il punto forte di tutta la narrativa di Zuboff.

(1)Mario Mancini, L'era del capitalismo della sorveglianza. L'oscura logica della nuova economia, in Medium, 2 marzo 2019, https://medium.com/@marioxmancini/lera-del-capitalismo-della-sorveglianza-68fe5403efa2

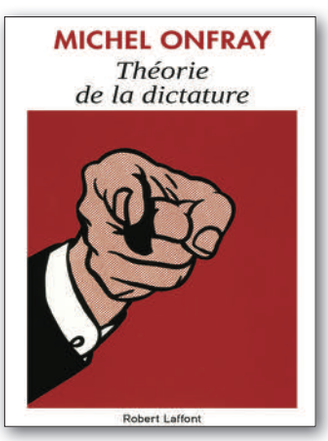
(2) Maurizio Franzini, Il capitalismo della sorveglianza secondo Shoshana Zuboff, in Eticaeconomia, 2 giugno 2019: www.eticaeconomia.it/il-capitalismo-della-sorveglianza-secondo-shoshana-zuboff/

(3) Hamilton Santia, Il capitalismo della sorveglianza esiste, e sta già cambiando le nostre vite, in Linkiesta, 7 novembre 2019: https://www.linkiesta.it/it/article/2019/11/07/capitalismo-sorveglianza-shoshanna-zuboff-recensione/44246/

(4) Il capitalismo di sorveglianza, recensione-conversazione, a cura di Géraldine Delacroix con l'economista Shoshana Zuboff sul suo nuovo libro The age of surveillance capitalism, in Effimera, 2 marzo 2019: http://effimera.org/capitalismo-sorveglianza-geraldine-delacroix/ ■

Michel Onfray, Théorie de la dictature. Précédé de Orwell et l'Empire maastrichtien, Paris, Robert Laffont, 2019, 615 pp.

Autore: Laurent Chrzanovski



Come per quasi tutte le opere di Michel Onfray anche questo saggio sarà disponibile a breve per i lettori italiani. E' stata annunciata, infatti, la pubblicazione per marzo 2020 dalla casa editrice "Ponte alle Grazie", motivo per il quale riteniamo importante presentarlo sin da subito. In Italia, finora, il saggio è stato acclamato dai media cattolici, specialmente per la parti che trattano la sessualità e il post/transumano, ma abbiamo trovato una interessantissima recensione, frutto della traduzione di un intervista ad Onfray da parte del giornalista belga Simon Brunfaut (1).

Agganciandoci a quanto scritto sull'awareness, e al capolavoro di Shoshanna Zuboff, l'ultimo nato dalla penna del filosofo francese è un vademecum sulla situazione attuale di degrado culturale, sociale, educativo, etico e morale del nostro continente, alla base dell'infiltrazione e l'implementazione completa, in Europa, del "capitalismo di sorveglianza" denunciato dalla Zuboff.

Michel Onfray fa opera di divulgazione utilissima ed accattivante, in uno stile semplice, limpido e provocatorio, come per tutti gli altri temi vitali per la società da lui trattati.

Non è un libro "denso" come quelli dove Onfray tratta di filosofi, bensì un manifesto con uno stile di stampa volutamente esagerato per far capire al meglio ogni idea: le pagine delle tesi orwelliane, di non più di due paragrafi, sono seguite da pagine che portano ognuna un esempio o un pensiero concreto, spesso di poche righe.

Questa innovazione è anche un'ironia voluta da Onfray, che ci regala un libro che, spesso, sembra una stampa di "tweets" individuali, a sottolineare la perdita della cultura e dell'arte della lettura cartacea, denunciata in molteplici passaggi del volume.

Nella lunga parte introduttiva *"Orwell et l'Empire maastrichien"*, Onfray ritraccia la storia dell'Unione Europea e ne denuncia, dallo stadio progettuale fino alla ratifica del trattato di Maastricht, l'ideologia sottostante.

La caccia frenetica ad un mercato unico di stampo (ultra)liberale, la creazione di una moneta indipendente dal fattore economico reale e della politica, rimasta prerogativa delle nazioni, sono, secondo l'autore, i semi che hanno permesso al nostro intero continente di diventare una sorta di appendice degli Stati Uniti, in variante ancora peggiore: *"in quasi un quarto di secolo, questo stato di Maastricht è diventato tossico quanto i regimi un tempo sostenuti da questi ex sessantottini - in questo senso, sono rimasti fedeli: amano le forme politiche che tengono i popoli al guinzaglio".*

È evidente l'abbandono della promessa di intercambio positivo tra le culture, di misure sociali, educative e miliari europee: *"è addirittura l'opposto della promessa che si realizzò: l'impoverimento galoppante, la proliferazione del razzismo e dell'antisemitismo, la partecipazione alle guerre atlantiste nel resto del pianeta, la distruzione degli equilibri nel Vicino e Medio Oriente, il crollo dei sistemi di protezione sociale e del servizio pubblico. Mai prima d'ora una promessa è stata a tal punto tradita".*

Questa prefazione è necessaria per capire che il mondo mostruoso, visto dagli Stati Uniti coll'occhio della Zuboff si realizza in modo ancora più nefasto, subdolo e senza speranza di miglioramento in un insieme di paesi sempre più deboli uniti in un sistema che non gestisce i piloni del reale potere (ovvero la gestione dei livelli di cultura, educazione, sanità, difesa e livello medio di benessere individuale e produttivo), rimasti prerogativa esclusiva di ogni governo.

Leggi diverse, mezzi diversi, politiche diverse in 28 Stati non hanno fatto altro, con l'aiuto della stessa Europa, «capo espiatorio» ma anche «boa di salvataggio» di ogni discorso governativo quando si tratta di misure poco popolari.

Da qui, Onfray ricorda la tesi di Orwell, spiegando, a seguito di ognuno dei dieci comandamenti di «1983», che stiamo già vivendo pienamente la sorveglianza dittatoriale che lo stesso Orwell predisse per il 2050.

Riprendiamo quindi a seguire il decalogo che assicura l'esercizio di una dittatura totalitaria 4.0, gestita da una ultra-minoranza globale che comporta «rappresentanti» e «agenti», tra politici, mediatici e scientifici, in ogni paese.

Il primo: distruggere la libertà - attivando così la polizia del pensiero, assicurando una sorveglianza perpetua, denunciando il crimine per pensiero, eliminando la solitudine, rallegrandosi delle vacanze obbligatorie, rovinando la vita personale.

Su questo punto, l'ingenuità e la crescente dipendenza di gran parte degli Europei ai social media e agli smartphone dispera Onfray. L'uomo europeo è "carnefice e vittima di sè stesso, martello e incudine di sè stesso, ferita e coltello della propria carne".

Estendendo il discorso al totalitarismo 4.0, che si nutre delle debolezze di ognuno di noi, aggiunge: *"Questa sorveglianza è la più riuscita di sempre, perché nessun regime totalitario avrebbe potuto sperare in qualcosa di meglio di un soggetto che, narcisismo ed egoismo, si fa indicatore di se stesso con giubilo, soddisfazione, piacere e gioia! Terenzio aveva teorizzato l'Heautontimoroumenos in un pezzo omonimo, Baudelaire ne aveva fatto un poema sublime, l'individuo postmoderno lo incarna."*

Continuando, il filosofo aggiunge: *"Tutte queste informazioni sono raccolte in una nuvola, il famoso i-cloud che ha sostituito gli angeli del cielo vuoto del Dio giudeo-cristiano. E' la cassaforte in cui mettiamo il furto che ci impegniamo ad offrire ai nostri ladri. Ci derubiamo costantemente a vantaggio di coloro che ci derubano per sfruttarci al meglio - il mondo dei GAFA".*

Il secondo: impoverire la lingua - praticando così una nuova lingua, usando lingua ambigua, parlando una sola lingua.

Quando osserviamo che bastano 200 parole per poter leggere un'edizione USA Today, e che il prestigioso Le Monde è passato in un decennio da 10'000 a meno di 2'000 parole, accettando e adottando tutti i neologismi di stampo anglosassone, capiamo ancora meglio la volontà nascosta di questa scelta, che vuol portarci tutti al "globish", l'esperanto americanizzato di oggi: *"Il processo di impoverimento del linguaggio è certamente una questione di parole, ortografia, grammatica, neologismi, acronimi, ma anche retorica. Prevenire tutto ciò che permette di ragionare, riflettere, pensare, pensare, concepire, speculare, è altrettanto importante quando il proprio progetto è quello di rendere un individuo completamente incolto."*

Il terzo: abolire la verità - diffondendo false notizie, cancellando il passato, producendo realtà.

Onfray è esplicito dall'inizio: *"Quando si annuncia la morte della verità, la bugia ha un viale. Grazie Foucault, grazie Deleuze. La generalizzazione dei social network ha dato massima visibilità alle menzogne, all'approssimazione, alla fiaba, alla bugia, alla propaganda, alla mistificazione, alla leggenda, alle favole, all'intossicazione. La logica non fa più legge. Nemmeno la ragione. E' responsabilità della persona che nega la menzogna dimostrare che non si tratta di una menzogna. Altrimenti, la menzogna diventa verità."*

Nel lungo capitolo, fa ridere, per non piangere, l'aneddoto che il filosofo ha inventato per spiegare meglio questa casistica: *"Dichiaro di aver passato la serata con un unicorno che mi ha parlato della sua vita sessuale. Il mio interlocutore dubita. Gli chiedo di dimostrarmi che la mia affermazione è falsa, anche se a priori irragionevole. Non riesce a farlo. Quindi concludo che ho ragione, che ha torto e che, di conseguenza, ho passato la serata con un unicorno... Posso anche aggiungere che dubitando che il mio interlocutore mi ha mancato di rispetto, e facendo mi ha insultato, un reato che richiede e giustifica un risarcimento. Altrimenti detto, posso prendere in mano la legge e colpire chiunque dubiti che io abbia passato la serata con un unicorno... Ecco dove ci troviamo in un paese che, per mezzo secolo, ha perso ogni legittimità per definirsi cartesiano..."*

Il quarto: sopprimere la storia - cioè fomentare l'odio, riscrivere la storia, distruggere i libri.

"La cancellazione del passato lascia un vuoto che deve essere riempito con la riscrittura del passato. Ciò che è successo non è esistito, ma ciò che non è mai successo è esistito - questo è l'obiettivo di questo lavoro di costruzione di un passato che non ha avuto luogo, di fare memoria di ciò che non è mai accaduto. Dove c'era sostanza, ora non c'è nulla; dove non c'era nulla, ora c'è sostanza."

"Il crollo della morale tradizionale, l'impunità per l'anonimato consentito dai social network, l'odio è diventato un luogo comune. Permette di evitare dibattiti, discussioni, scambi e controversie a solo vantaggio del discredito della persona. La logica del capro espiatorio è in cima alla lista. Tuttavia, chiunque sia in preda all'odio, individui o persone, Stati o nazioni, non pensa più. Scollegato dal suo sistema neurale, è collegato al suo sistema neurovegetativo. La corteccia viene licenziata, il cervello rettiliano fa da apripista. Il nostro tempo è un tempo di odio."

In queste due affermazioni, Onfray raggiunge l'ultimo libro del rimpianto Zygmunt Bauman, Retrotopia (2), dove il sociologo polacco ritrova la creazione e la diffusione della propaganda di una falsa storia nazionale piena di gloria, e quindi il rimpianto per "periodi d'oro" mai esistiti ma che i governi e partiti che ne fanno grande uso vorrebbero far rinascere…

Il quinto: negare la natura - quindi negare le leggi della natura, imporre un corpo igienico, procreare medicalmente.

Un solo esempio reale, come una sfida totale a qualsiasi etica e morale occidentale, illustra da solo l'intero capitolo: *"Nell'edizione del 30 marzo 2019, il Daily Mail riporta che negli Stati Uniti (Nebraska), una donna di 61 anni ha dato alla luce una bambina concepita con lo sperma del figlio e l'ovulo della sorella del marito del figlio. La madre che ha partorito questo bimbo è quindi anche sua nonna, ma questa nipote ha anche sua zia come madre, il che gli conferisce quattro genitori, il tutto nella logica incestuosa più perfetta, poiché la madre viene inseminata dal seme del proprio figlio. Se anche questa zia dovesse essere padre, i figli sarebbero cugini allo stesso tempo dei fratellastri o delle mezze sorelle."* E di concludere cinicamente: *"Se la logica incestuosa deve essere il segno più progressista del progressismo possiamo capire che non sottoscriviamo questo tipo di progresso..."*

Il sesto: artificializzare i corpi - distruggere il piacere di vivere, procreare medicalmente, organizzare la frustrazione sessuale.

Proprio partendo dall'esempio precedente, Onfray denuncia il "politically correct" imposto dalla censura dei GAFAM. La nascita del bimbo suscitò non pochi commenti, molti immediatamente eliminati dai nuovi "censori morali" planetari perché giudicati omofobi o anti-progressisti. In questo quadro, ha perfettamente ragione Onfray quando denuncia che *"Se il genere e la razza non esistono, non può esistere nemmeno la lotta contro la discriminazione di genere o la discriminazione razziale. Le differenze razziali sia sessuali che naturali non portano di fatto a disuguaglianze di genere o razziali. La differenza naturale diventa una disuguaglianza nel registro culturale solo dopo che la discriminazione è stata stabilita tra due istanze separate e convalidata da prove empiriche."*

Peggio, il frutto della società digitale ambigua e ambivalente, messa al di fuori di ogni morale o etica precedente da messaggi scientificamente distillati dai social, *"L'uomo è considerato al di fuori dei cicli naturali, dei cicli stagionali, dei cicli solari e lunari, dei cicli cosmici. Figlio del cemento e dell'asfalto, figlio delle città e del cemento, produce biblioteche e, più recentemente, flussi digitali. La questione del sesso, del genere, non è più una questione di natura, ma di cultura."*

Il settimo: rovinare la cultura - riassegnare ad altri usi i luoghi di culto, industrializzare le produzioni artistiche, abbassare l'educazione del popolo, disinformare i bambini, sopprimere la bellezza.

Qui, Onfray porta un'idea nuova, che in effetti invade il mondo digitale: *"La natura si oppone alla cultura, la prima sciocchezza che ci impedisce di pensare. Più alta sarebbe la prima, più piccola sarebbe l'altra: un essere naturale si rivelerebbe ruvido e semplice, se non semplicistico e idiota, se non fosse il cannibale di Montaigne o il buon selvaggio di Rousseau. Un essere colto è ornato con le piume del più bel pavone. La cultura non è in natura, quindi non si trova in campagna, ma nelle città. E' urbano. Questa pietrificazione delle anime, questa bitumizzazione delle intelligenze, questa cementazione della ragione contribuiscono alla cancellazione della natura, che è ormai considerata solo nella configurazione dell'ecologia urbana e in modo antropico: secondo questa visione del mondo urbano-centrico, l'uomo rimane al centro della natura, ne è padrone e proprietario. Se il pianeta si sta riscaldando, è solo colpa sua."*

Secondo Onfray, solo la natura, il bene ed il male che gli fanno subire l'uomo sono ormai vera cultura, permettendo di gettare all'oblio letteratura, arte, filosofia e tutto ciò che permette di riflettere

L'ottavo: fomentare le guerre - quindi: creare un nemico, mantenere le guerre.

Onfray, qui, non stupisce gli esperti di strategia e viene ad assecondare i rapporti dell'ONU secondo i quali i conflitti armati – anche se molti di essi sono geograficamente minori – sono cresciuti in modo drammatico dalla fine della guerra fredda. E condanna l'ignoranza voluta dei conflitti nei quali non vi è interesse monetario ad ugual modo che la disproporzione di vocaboli e trattamento dei conflitti dove i nostri Stati sono "i buoni" e tutti gli altri…

"In un mondo in cui l'odio è stato propagato dai progressisti, il progresso è il seguente per credere che si pensa solo quando si odia, è cercarsi un nemico senza il quale non si può vivere; è mantenere passioni tristi come viatico; è psichiatrizzare il pensiero critico e sporcare chiunque non pensi come se stesso piuttosto che criticare le sue argomentazioni. È giustificare le guerre e difenderle quando vengono dichiarate, ma condannarle quando altri prendono l'iniziativa; è far finta di essere sorpresi che il terrorismo si presenta come una risposta dal debole al forte; è lodare la pace facendo commercio di armi e giustificandone l'uso nei campi di battaglia dove ci si invita oppure che noi stessi creiamo".

Il nono: aspirare all'Impero - quindi: governare con le élite, praticare l'urbanistica di classe; amministrare l'opposizione, psichiatrizzare ogni pensiero critico, nascondere il potere.

I misfatti dell'urbanistica 'di classse', che si vedono nelle periferie francesi e nel loro stato di degrado permanente, servono ad Onfray ad aprire uno scenario globale dove questi veri e propri ghetti diventeranno la norma, siccome *"La proprietà, ad esempio, non è più nelle mani di singoli individui, ma di gruppi. La missione dell'élite, composta da giornalisti e intellettuali, pubblicitari e sindacalisti, burocrati e politici, sociologi e professori, tecnici e scienziati, è quindi quella di perpetuare la confiscazione dei beni, delle ricchezze e delle proprietà dei singoli individui per affidarli alle mani di gruppi che, a loro volta, permettono ai membri di questa oligarchia di vivere una vita di nababbi. Per questo motivo le disuguaglianze economiche sono diventate permanenti."*

Il decimo: cancellare l'uomo - quindi: dominare attraverso il progresso, realizzare l'ultimo uomo.

Per Onfray, *"Il mondo dei GAFA non nasconde il suo progetto: realizzare il postumano, superare l'uomo, per finire con questa vecchia luna. Questo porta anche all'abolizione delle civiltà e dei Divers cari a Segalen, a beneficio di un mondo unito, unito, unito, unificato. La GAFA rivendica un'ideologia attivata da un'élite con denaro illimitato, e quindi potere assoluto. Ogni clic planetario è una moneta d'oro nella loro escarcelle. Attirano scienziati, ricercatori, ingegneri, informatici, biologi, biologi, biologi, chirurghi, scienziati cognitivi, programmatori, cibernetici, astrofisici, neurologi, filosofi, sociologi, per realizzare una chimera che unisce il corpo biologico e la carne digitale."*

Ed è proprio qui che Onfray porta il dibattito ben oltre Zuboff: il vero e proprio pericolo parastatale delle GAFAM, non controllate da nessuno, è quello di ambire a creare una società ibrida tecno-umana, asessuata e amorale, ideale.

Insiste proprio su questo punto perché la fase attuale, quella del condizionamento dei cervelli tramite l'intossicazione informazionale (per straordinaria quantità e sempre più mediocre qualità) sta già portando i suoi frutti e che, nel frattempo, le stesse majors investono somme colossali in tutte le scienze relative all'anatomia e alla natura, essendo recentemente riuscite ad impiantare ricordi artificiali nel cervello di ratti in laboratorio, senza nessun ostacolo legale.

Onfray, più che mai, è da leggere imperativamente. Certo, la sua scarsa domesticità con le lingue ma anche la sua onestà limita i numerosissimi esempi del paese nel quale vive ed a fatti noti e provati, maggioritariamente statunitensi. Proprio per questo, ma molto più "arido", va affiancato e completato dai due ultimi volumi di Slavoj Žižek: per i GAFAM, *Come un ladro in pieno giorno. Il potere all'epoca della postumanità* (appena tradotto in Italiano, ed. Ponte alle Grazie, Milano 2019) e per la tendenza all'essere trans/postsessuale: Sex and the Failed Absolute, Bloomsbury Academic 2019.

(1) "La cretinizzazione progressiva della gente rappresenta un vero problema" (Intervista a Michel Onfray) https://comedonchisciotte.org/la-cretinizzazione-progressiva-della-gente-rappresenta-un-vero-problema-intervista-a-michel-onfray/

(2) Zygmunt Bauman, Retrotopia, ed. orig. 2017, trad. dall'inglese di Marco Cupellaro, Laterza, Bari-Roma 2017, 206 pp. ■

Una pubblicazione

web for business
swiss webacademy

A cura del

Global Cyber Security Center

Nota copyright:
Copyright © 2019 Swiss WebAcademy e GCSEC.
Tutti diritti riservati
I materiali originali di questo volume appartengono a SWA ed al GCSEC.

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
www.cybertrends.it

CERT STAR

*Il **CERT STAR** è un programma di incontri a porte chiuse dedicato ai **CERT** e ai **SOC** italiani volto ad alimentare le **competenze**, promuovere la **cooperazione** e la **condivisione** di esperienze. Nel corso degli incontri sono analizzate a livello **tecnico operativo** le principali **tematiche "core"** dei team di security.*

PROGRAMMA 2020

- INCONTRI **Milano e Roma**
- VISITE **CERT Internazionale**
- PRACTICAL CTF **Capture the Flag**
- TEORICAL SESSIONS **Metodologie e Studi**
- TRAINING SESSIONS **Hands-On**

GLOBAL CYBER SECURITY CENTER

Per maggiori informazioni scrivere a
info@gcsec.org

Il primo Tool per valutare il livello di maturità del tuo CERT e dei suoi Servizi

Available Soon

www.certrating.it

Per maggiori dettagli
Info@gcsec.org